

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP2006/313347

International filing date: 28 June 2006 (28.06.2006)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2005-189053
Filing date: 28 June 2005 (28.06.2005)

Date of receipt at the International Bureau: 03 August 2006 (03.08.2006)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2005年 6月28日

出 願 番 号
Application Number: 特願2005-189053

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

J P 2005-189053

出 願 人
Applicant(s): 株式会社東芝
東芝ソリューション株式会社

2006年 7月19日

特許庁長官
Commissioner,
Japan Patent Office

中 嶋



【書類名】 特許願
【整理番号】 13B0560411
【提出日】 平成17年 6月28日
【あて先】 特許庁長官殿
【国際特許分類】 G11B 20/10
G06F 12/14

【発明者】
【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝 研究開発
センター内
【氏名】 磯崎 宏

【発明者】
【住所又は居所】 東京都府中市片町 3 - 2 2
【氏名】 松川 伸一

【発明者】
【住所又は居所】 神奈川県横浜市磯子区新杉田町 8 番地 株式会社東芝 横浜事業
所内
【氏名】 石原 淳

【発明者】
【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝 研究開発
センター内
【氏名】 加藤 拓

【特許出願人】
【識別番号】 000003078
【氏名又は名称】 株式会社東芝

【特許出願人】
【識別番号】 301063496
【氏名又は名称】 東芝ソリューション株式会社

【代理人】
【識別番号】 100089118
【弁理士】
【氏名又は名称】 酒井 宏明

【手数料の表示】
【予納台帳番号】 036711
【納付金額】 16,000円

【提出物件の目録】
【物件名】 特許請求の範囲 1
【物件名】 明細書 1
【物件名】 図面 1
【物件名】 要約書 1

【書類名】特許請求の範囲

【請求項1】

番組の映像または音声のコンテンツである複数のタイトルコンテンツをタイトルコンテンツごとに暗号化する1つ以上のタイトルキーが登録されたタイトルキーファイルと、前記タイトルキーによって暗号化されたタイトルコンテンツとが記録された記録媒体の記録および再生を行うコンテンツ記録再生装置であって、

前記タイトルキーファイルの一つ以上を生成し、一つ以上の前記タイトルキーを、生成された前記タイトルキーファイルに格納する初期化手段と、

複数のタイトルキーファイルのそれぞれに対応した第1の乱数を生成する第1の乱数生成手段と、

複数のタイトルキーファイルのそれぞれに対応した第2の乱数を生成する第2の乱数生成手段と、

前記初期化手段によって生成された前記タイトルキーファイルと前記第1の乱数と組にしてそれぞれ前記記録媒体に記録する記録手段と、を備え、

前記初期化手段は、前記複数のタイトルキーファイルのそれぞれを、前記第1の乱数生成手段によって生成され、前記タイトルキーファイルに対応した前記第1の乱数と関連付けられた他のタイトルキーファイルに登録された前記第2の乱数とによって前記タイトルキーを暗号化した暗号化タイトルキーと、前記タイトルキーファイルに対応した前記第1の乱数と前記他のタイトルキーファイルに登録された前記第2の乱数とを登録することによって生成することを特徴とするコンテンツ記録再生装置。

【請求項2】

前記記録媒体から前記複数のタイトルキーファイルを読み出す読み出し手段と、

前記記録媒体に記録された前記タイトルキーのリストに、新たなタイトルキーが追加された場合または前記タイトルキーのリストからタイトルキーが削除された場合に、前記読み出し手段によって読み出した前記複数のタイトルキーファイルの中で任意の前記タイトルキーファイルに登録された前記第1の乱数と前記タイトルキーファイルに関連付けられた他の前記タイトルキーファイルに登録された前記第2の乱数によって前記タイトルキーファイルに登録された前記暗号化タイトルキーを復号化し、前記第2の乱数を前記第2の乱数生成手段によって前記複数のタイトルキーファイルごとに新たに生成し、復号化された前記タイトルキーを、前記第1の乱数生成手段によって新たに生成された前記第1の乱数と他の前記タイトルキーファイルに対応して新たに生成された前記第2の乱数とによって前記タイトルキーファイルを暗号化する再暗号化手段と、

前記暗号化タイトルキーと前記第1の乱数と前記第2の乱数とを登録した前記タイトルキーファイルを複数生成することにより、前記複数のタイトルキーファイルを更新する更新手段と、をさらに備え、

前記記録手段は、前記更新手段によって更新された前記複数のタイトルキーファイルを前記記録媒体に記録することを特徴とする請求項1に記載のコンテンツ記録再生装置。

【請求項3】

前記記録媒体に記録された前記複数のタイトルキーファイルの中で、一つの前記タイトルキーファイルが存在しない場合あるいは破壊されている場合に、前記記録媒体に存在している前記タイトルキーファイルに登録された前記第1の乱数と前記タイトルキーファイルに関連付けられた他の前記タイトルキーファイルに登録された前記第2の乱数によって前記タイトルキーファイルに登録された前記暗号化タイトルキーを復号化し、前記第2の乱数を前記複数のタイトルキーファイルごとに新たに生成し、復号化された前記タイトルキーを、前記第1の乱数生成手段によって新たに生成された前記第1の乱数と他の前記タイトルキーファイルに対応して新たに生成された前記第2の乱数とによって暗号化する第2の再暗号化手段と、

前記暗号化タイトルキーと前記第1の乱数と前記第2の乱数とを登録した前記タイトルキーファイルを複数生成することによって、前記複数のタイトルキーファイルを回復する回復手段をさらに備え、

前記記録手段は、前記回復手段によって回復された前記複数のタイトルキーファイルを前記記録媒体に記録することを特徴とする請求項2に記載のコンテンツ記録再生装置。

【請求項4】

前記記録媒体は、任意の値を書き込むことが不可能なプロテクト領域と、任意のアプリケーションにより任意の値が記録可能なユーザ領域とを備え、

前記記録手段は、前記タイトルキーファイルの前記第1の乱数をプロテクト領域に記録し、前記第2の乱数を前記ユーザ領域に記録し、前記タイトルキーファイル以外のファイルを記録する場合には、前記プロテクト領域に正当な記録でない旨を示す不当情報を前記第1の乱数として記録する記録手段であって、

前記回復手段は、前記暗号化タイトルキーを復号化する際に、前記第1の乱数に前記不当情報が記録されているか否かを判断し、前記不当情報が記録されている場合には、前記複数のタイトルキーファイルの回復を行わないことを特徴とする請求項3に記載のコンテンツ記録再生装置。

【請求項5】

番組の映像または音声のコンテンツである複数のタイトルコンテンツをタイトルコンテンツごとに暗号化する1つ以上のタイトルキーが登録されたタイトルキーリストと、前記タイトルキーによって暗号化されたタイトルコンテンツとが記録された記録媒体の記録および再生を行うコンテンツ記録再生方法であって、

前記タイトルキーファイルを一つ以上生成し、一つ以上の前記タイトルキーを、生成された前記タイトルキーファイルに格納し、前記記録媒体に記録する初期化ステップと、

複数のタイトルキーファイルのそれぞれに対応した第1の乱数を生成する第1の乱数生成ステップと、

複数のタイトルキーファイルのそれぞれに対応した第2の乱数を生成する第2の乱数生成ステップと、

前記初期化ステップによって生成された前記タイトルキーファイルと前記第1の乱数とを組にしてそれぞれを前記記録媒体に記録する記録ステップと、を含み、

前記初期化ステップは、前記複数のタイトルキーファイルのそれぞれを、前記第1の乱数生成ステップによって生成され、前記タイトルキーファイルに対応した前記第1の乱数と関連づけられた他のタイトルキーファイルに登録された前記第2の乱数とによって前記タイトルキーを暗号化した暗号化タイトルキーと、前記タイトルキーファイルに対応した前記第1の乱数と前記他のタイトルキーファイルに登録された前記第2の乱数とを登録することによって生成することを特徴とするコンテンツ記録再生方法。

【請求項6】

番組の映像または音声のコンテンツである複数のタイトルコンテンツをタイトルコンテンツごとに暗号化する1つ以上のタイトルキーが登録されたタイトルキーリストと、前記タイトルキーによって暗号化されたタイトルコンテンツとが記録された記録媒体の記録および再生を行うコンテンツ記録再生プログラムであって、

前記タイトルキーファイルを一つ以上生成し、一つ以上の前記タイトルキーを、生成された前記タイトルキーファイルに格納し、前記記録媒体に記録する初期化ステップと、

複数のタイトルキーファイルのそれぞれに対応した第1の乱数を生成する第1の乱数生成ステップと、

複数のタイトルキーファイルのそれぞれに対応した第2の乱数を生成する第2の乱数生成ステップと、

前記初期化ステップによって生成された前記複数のタイトルキーファイルと前記第1の乱数とを組にしてそれぞれを前記記録媒体に記録する記録ステップと、をコンピュータに実行させ、

前記初期化ステップは、前記複数のタイトルキーファイルのそれぞれを、前記第1の乱数生成ステップによって生成され、前記タイトルキーファイルに対応した前記第1の乱数と関連づけられた他の前記タイトルキーファイルに登録された前記第2の乱数とによって前記タイトルキーファイルを暗号化した暗号化タイトルキーと、前記タイトルキーファイ

ルに対応した前記第 1 の乱数と前記他のタイトルキーファイルに登録された前記第 2 の乱数とを登録することによって生成することを特徴とするコンテンツ記録再生プログラム。

【書類名】明細書

【発明の名称】コンテンツ記録再生装置、コンテンツ記録再生方法およびコンテンツ記録再生プログラム

【技術分野】

【0001】

本発明は、番組の映像または音声のコンテンツである複数のタイトルコンテンツをタイトルコンテンツごとに暗号化する複数のタイトルキーが登録されたタイトルキーファイルと、前記タイトルキーによって暗号化されたタイトルコンテンツとが記録された記録媒体の記録および再生を行うコンテンツ記録再生装置、コンテンツ記録再生方法およびコンテンツ記録再生プログラムに関し、特にタイトルキーファイルのバックアップ技術に関するものである。

【背景技術】

【0002】

従来から、DVD (Digital Versatile Disk) 等の記録媒体に記録されたコンテンツの不正コピーを防止するため、番組の映像または音声のコンテンツである複数のタイトルコンテンツのそれぞれに対して、タイトルコンテンツごとに異なるタイトルキーで暗号化処理を施して、暗号化されたタイトルコンテンツをDVDメディアに記録する技術が知られている（例えば、非特許文献1参照）。

【0003】

この技術では、複数のタイトルキーのそれぞれを、コンテンツを正当に記録再生するDVDレコーダ等の記録再生装置ごとに付与されたデバイスキーとランダムに発生させた乱数とにより暗号化して乱数とともにタイトルキーファイルに登録してDVDメディアに記録している。そして、タイトルコンテンツを再生する場合には、このタイトルキーファイルに登録されている暗号化タイトルキーを乱数と再生しようとする記録再生装置のデバイスキーで復号化して復号化されたタイトルキーでタイトルコンテンツを復号化してタイトルコンテンツを再生している。

【0004】

また、書き換え型のDVDメディアにおいてタイトルコンテンツの一部を削除した場合には、タイトルキーファイルも更新する。具体的には、一度、タイトルキーファイルを復号化し、新たに乱数を生成し、デバイスキーでDVDメディアから削除したタイトルコンテンツに対応するタイトルキーを削除したタイトルキーファイルを、新たな乱数とデバイスキーにより再度暗号化してDVDメディアに記録している。これによって、削除したタイトルコンテンツに対応するタイトルキーを予め複製しておき、このタイトルキーを用いて削除したタイトルコンテンツを不正に再生する攻撃を防止することができる。

【0005】

【非特許文献1】Advanced Access Content System (AACs) Recordable Video Book
Revision 0.90

【発明の開示】

【発明が解決しようとする課題】

【0006】

このようなタイトルキーを用いたコンテンツ保護は、DVDメディアのコンテンツの不正利用を防止するために有効な技術であるが、DVDメディアの汚れや傷等により一部の領域が読み出し不可能となり、タイトルキーファイルの読み出しができなくなった場合や、ユーザが誤ってタイトルキーファイルを消去してしまった場合には、タイトルコンテンツの復号化ができなくなり再生不可能となってしまう。このため、タイトルキーファイルの複製をバックアップファイルとしてDVDメディアに記録しておき、タイトルキーファイルが壊れた等で読み出すことができない場合には、バックアップファイルをタイトルキーファイルとして使用することが考えられる。

【0007】

しかしながら、タイトルキーファイルの単純なバックアップファイルをDVDメディア

に記録しておくだけでは、コンテンツの不正な復元を許容してしまうことになる。すなわち、例えば、攻撃者が予めタイトルキーファイルのバックアップファイルを他のメディアにコピーしておいたとする。このとき、正規の手順でタイトルコンテンツの一部を他のメディアに移動した場合には、移動したタイトルコンテンツに対するタイトルキーを削除したタイトルキーファイルが更新される。このとき、攻撃者は、タイトルキーファイルをDVDメディアから削除し、当該DVDメディアに他のメディアにコピーしておいたバックアップファイルを復元する。すると、記録再生装置は、本来のタイトルキーファイルがDVDメディアに存在しないため、タイトルキーファイルをバックアップから復元するが、このバックアップファイルは更新前のタイトルキーファイルであるため、DVDメディアから削除したはずのタイトルコンテンツに対するタイトルキーが不正に復元されてしまうことになる。

【0008】

本発明は、上記に鑑みてなされたものであって、タイトルキーファイルの復元を確実に行えるとともに、悪意のある第三者によるコンテンツの不正な復元を防止することができるコンテンツ記録再生装置、コンテンツ記録再生方法およびコンテンツ記録再生プログラムを提供することを目的とする。

【課題を解決するための手段】

【0009】

上述した課題を解決し、目的を達成するために、本発明は、番組の映像または音声のコンテンツである複数のタイトルコンテンツをタイトルコンテンツごとに暗号化する1つ以上のタイトルキーが登録されたタイトルキーファイルと、前記タイトルキーによって暗号化されたタイトルコンテンツとが記録された記録媒体の記録および再生を行うコンテンツ記録再生装置であって、前記タイトルキーファイルを一つ以上生成し、一つ以上の前記タイトルキーを、生成された前記タイトルキーファイルに格納する初期化手段と、複数のタイトルキーファイルのそれぞれに対応した第1の乱数を生成する第1の乱数生成手段と、複数のタイトルキーファイルのそれぞれに対応した第2の乱数を生成する第2の乱数生成手段と、前記初期化手段によって生成された前記タイトルキーファイルと前記第1の乱数と組にしてそれぞれ前記記録媒体に記録する記録手段と、を備え、前記初期化手段は、前記複数のタイトルキーファイルのそれぞれを、前記第1の乱数生成手段によって生成され、前記タイトルキーファイルに対応した前記第1の乱数と関連づけられた他のタイトルキーファイルに登録された前記第2の乱数とによって前記タイトルキーを暗号化した暗号化タイトルキーと、前記タイトルキーファイルに対応した前記第1の乱数と前記他のタイトルキーファイルに登録された前記第2の乱数とを登録することによって生成することを特徴とする。また、本発明は、上記装置に対応したコンテンツ記録再生方法およびプログラムである。

【発明の効果】

【0010】

本発明によれば、タイトルキーファイルを複数生成し、各タイトルキーファイルは、互いに他のタイトルキーファイルと関連付けされているため、タイトルキーファイルの復元を確実に行えるとともに、悪意のある第三者によるコンテンツの不正な復元を防止することができるという効果を奏する。

【発明を実施するための最良の形態】

【0011】

以下に添付図面を参照して、コンテンツ記録再生装置、コンテンツ記録再生方法およびコンテンツ記録再生プログラムの最良な実施の形態を詳細に説明する。

【0012】

（実施の形態1）

図1は、実施の形態1にかかるコンテンツ記録再生装置100の構成を示すブロック図である。ここで、コンテンツ記録再生装置100としては、例えば、DVDメディアへの記録および再生を行うDVDレコーダ等があげられる。本実施の形態にかかるコンテンツ

記録再生装置100は、図1に示すように、書き換え可能なDVDメディア140にデータの機器録およびDVDメディア140からのデータの読み出し等を行うドライブ部110と、タイトルコンテンツの暗号化と復号化およびタイトルキーファイル（TKF：Title Key File）のバックアップ処理を行うホスト部120がバス130で接続された構成となっている。

【0013】

DVDメディア140には、図1に示すように、後述するタイトルキーファイル（TKF#1）、タイトルキーファイルのバックアップファイルであるTKF#2、TKF#3、乱数1～3が記録されている。

【0014】

ここで、本実施の形態のコンテンツ記録再生装置100で対象としているDVDメディア140の形式は、HD DVD（High Density Digital Versatile Disk）Video Recording規格に準拠したDVDメディアであるが、必ずしもかかるフォーマットのDVDメディアに限定されるものではない。

【0015】

ドライブ部110は、ランダムに乱数を生成する乱数生成部111と、DVDメディア140からデータを直接読み出す読み出し部112と、DVDメディア140に対して、データを直接記録する記録部113とを主に備えている。

【0016】

ホスト部120は、図1に示すように、コンテンツ暗号化処理部121と、コンテンツ復号化処理部122と、TKF暗号化処理部123と、デバイス秘密鍵記憶部124と、バックアップ処理部140と、乱数生成部125を主に備えた構成となっている。

【0017】

コンテンツ暗号化処理部121は、タイトルキーコンテンツをタイトルキーによって暗号化する処理部であり、コンテンツ復号化処理部122は、暗号化されたタイトルコンテンツをタイトルキーによって復号化する処理部である。

【0018】

ここで、タイトルコンテンツは、番組としての映像や音声のコンテンツの単位であり、例えば、映画一本のコンテンツが一つのタイトルコンテンツとなる。タイトルキーは、このタイトルコンテンツを暗号化する鍵であり、タイトルコンテンツごとに異なる鍵となっている。なお、複数のタイトルが同一のタイトルキーで暗号化されていてもよい。

【0019】

TKF暗号化処理部123は、タイトルキーファイル（TKF）を暗号化する処理部である。ここで、タイトルキーファイル（TKF）は、1つ以上のタイトルキーを乱数とコンテンツ記録再生装置100が有するデバイス秘密鍵とによって暗号化した1つ以上のタイトルキーの集合であり、かかるタイトルキーの集合と暗号化の際に使用した乱数が登録されたファイルである。タイトルキーファイルは、後述する乱数と、自身のタイトルキーファイルまたはバックアップファイル以外のファイルの暗号化されたタイトルキーを生成するためのTKF乱数と、1つ以上の暗号化されたタイトルキーとが登録されており、DVDメディア140に記録される。タイトルキーファイルの詳細は図4-1および図4-2にて後述する。

【0020】

図1に戻り、デバイス秘密鍵記憶部124は、デバイス秘密鍵を記憶するメモリ等の記憶媒体である。ここで、デバイス秘密鍵とは、正規のコンテンツ記録再生装置100に対して予め付与された秘密鍵であり、タイトルキーファイルのタイトルキーを暗号化および復号化するための鍵となっている。

【0021】

TKFバックアップ処理部140は、DVDメディア140に記録されているタイトルキーファイル（TKF）のバックアップ処理を行う処理部であり、TKF初期化部141と、TKF更新部142と、TKF回復部143とを主に備えている。

【0022】

TKF初期化部141は、DVDメディア140に記録されたタイトルキーファイル（TKF#1）とバックアップファイルとしてのタイトルキーファイルTKF#2、TKF#3を生成する処理部である。

【0023】

TKF更新部142は、DVDメディア140のタイトルコンテンツの一部が削除または追加となり、タイトルキーのリストに変更が起こった場合に、タイトルキーファイルが更新されるが、これに伴って、タイトルキーファイルTKF#1とバックアップファイルとしてのタイトルキーファイルTKF#2、TKF#3を再生成して更新する処理部である。

【0024】

TKF回復部143は、DVDメディア140のタイトルキーファイルTKF#1またはバックアップファイルとしてのタイトルキーファイルTKF#2、TKF#3のうち、どれか一つが破壊されていた場合、あるいは存在しなかった場合に、タイトルキーファイルTKF#1、バックアップファイルとしてのタイトルキーファイルTKF#2、TKF#3の中の一つからタイトルキーを再生してタイトルキーファイルおよびバックアップファイルとしてのタイトルキーファイルを回復する処理部である。乱数生成部125は、後述するTKF乱数を生成する処理部である。

【0025】

次に、DVDメディア140のデータを構成するセクタの構造について説明する。データは、セクタと呼ばれる固定長のデータに分割されて、DVDメディア140に記録されている。そして、DVDメディア140上のあらゆるデータは、セクタ単位に読み出しおよび書き込みが行われる。図2は、セクタの構造を示す説明図である。1セクタは、図2に示すように、固定長Mバイトの管理用のセクタヘッダとNバイトのデータとから構成される。そして、データは、任意のアプリケーションでリードライト可能なユーザ領域に記録され、セクタヘッダの一部は、外部から任意の値をライトできないプロテクト領域に記録される。外部から任意の値をライトできないようにする仕組みとして、図3に示すようなプロトコルを用いればよい。図3は、乱数をDVDメディア140に書き込む処理の手順を示すシーケンス図である。

【0026】

まず、ホスト部120からドライブ部110に乱数生成命令が送信される（ステップS301）。この乱数生成命令を受信したドライブ部110では乱数生成部111により乱数を生成し（ステップS302）、生成した乱数を一時的に蓄積しておく。次に、ホスト部120はドライブ部110に乱数書き込み命令を送信する（ステップS303）。ここで、乱数書き込み命令には乱数の値は含まれていない。数書き込み命令を受信したドライブ部110では、一次蓄積しておいた乱数を記録部113によってDVDメディア140に書き込む（ステップS304）。このように、乱数書き込み命令に乱数の値を含まないようにすることで、ドライブ部110が生成した値以外の値をDVDメディア140に書き込むことを防ぐことができる。

【0027】

次に、本実施の形態のタイトルキーファイルのバックアップについて説明する。図4-1は、実施の形態1のタイトルキーファイルとバックアップファイルとしてのタイトルキーファイルの構造を示す説明図である。なお、以下においては説明の都合上、バックアップファイルとしてのタイトルキーファイルTKF#2、TKF#3を単にバックアップファイルTKF#2、TKF#3という。本実施の形態では、TKF初期化部141によって、DVDメディア140に記録されたタイトルキーファイル（TKF#1）のバックアップファイルをTKF#2、TKF#3として生成し、この3つのTKF#1、TKF#2、TKF#3をドライブ部110の記録部113によってDVDメディア140に格納している。

【0028】

タイトルキーファイル (TKF # 1) と各バックアップファイル TKF # 2, TKF # 3 は、乱数 1 ~ 3 (BN 1, BN 2, BN 3) と、世代と、TKF 乱数 1 ~ 3 と、暗号化タイトルキー (ETK 1 ~ 3) とを登録した構成となっている。乱数 1 ~ 3 (BN 1, BN 2, BN 3) は、ホスト部 1 2 0 の要求を受けてドライブ部 1 1 0 の乱数生成部 1 1 1 によってランダムに生成されてドライブ部 1 1 0 の記録部 1 1 3 によって DVD メディア 1 4 0 上に記録される。世代は、タイトルキーファイル (TKF # 1) およびバックアップファイル TKF # 2, TKF # 3 の変更回数を示すものである。

【0029】

TKF 乱数 1 ~ 3 (TKFN 1, TKFN 2, TKFN 3) は、自身のタイトルキーファイルまたはバックアップファイル以外のファイルの暗号化タイトルキー (ETK 1, ETK 2, ETK 3) を生成するための乱数である。TKF 乱数 1 ~ 3 はホスト部 1 2 0 の乱数生成部 1 2 5 によって生成される。

【0030】

暗号化タイトルキー (ETK 1, ETK 2, ETK 3) は、タイトルキーファイルまたはバックアップファイルに登録されている乱数 1 ~ 3 (BN 1, BN 2, BN 3) と、関連づけされている他のファイルに登録されている TKF 乱数 1 ~ 3 (TKFN 1, TKFN 2, TKFN 3) によって、タイトルキーファイルの全タイトルキーを暗号化したデータである。図 4-2 は、暗号化タイトルキー (ETK 1, ETK 2, ETK 3) の構造を示す説明図である。(ETK 1, ETK 2, ETK 3) は、図 4-2 に示すように、タイトルキー 1 ~ n のそれぞれを暗号化したものとなっている。暗号化タイトルキー (ETK 1, ETK 2, ETK 3) は、次の (1) ~ (3) 式で示される。

【0031】

$$ETK1 = I(TK, BN1, TKFN3) \quad \dots (1)$$

$$ETK2 = I(TK, BN2, TKFN1) \quad \dots (2)$$

$$ETK3 = I(TK, BN3, TKFN2) \quad \dots (3)$$

ここで、TK は平文のタイトルキーを示し、I は、第 1 パラメタ (TK) に第 2 パラメタ (BN 1 ~ 3) と第 3 パラメタ (TKFN 1 ~ 3) を暗号鍵として暗号処理を施すことを示している。暗号処理 I には、たとえば AES (Advanced Encryption Standard) などのよく知られた暗号アルゴリズムを用いればよい。

【0032】

すなわち、TKF # 1 は、TKF # 3 と関連づけられており、タイトルキー (TK) を、乱数 1 (BN 1) と、関連づけられた TKF # 3 の TKF 乱数 3 (TKFN 3) とで暗号化したものとなっている。また、TKF # 2 は、TKF # 1 と関連づけられており、タイトルキー (TK) を、乱数 2 (BN 2) と、関連づけられた TKF # 1 の TKF 乱数 1 (TKFN 1) とで暗号化したものとなっている。さらに、TKF # 3 は、TKF # 2 と関連づけられており、タイトルキー (TK) を、乱数 3 (BN 3) と、関連づけられた TKF # 2 の TKF 乱数 2 (TKFN 2) とで暗号化したものとなっている。

【0033】

このようにタイトルキーファイル TKF # 1 と各バックアップファイル TKF # 2, TKF # 3 は、互いに他のファイルと関連付けられており、暗号化タイトルキー (ETK 1, ETK 2, ETK 3) は、自己のファイルに登録された乱数 1 ~ 3 (BN 1, BN 2, BN 3) と、関連づけられている他のファイルに登録されている TKF 乱数 1 ~ 3 (TKFN 1, TKFN 2, TKFN 3) とでタイトルキー (TK) を暗号化したものとなっているので、悪意のある第三者が一つのバックアップファイルをコピーしてもタイトルキー (TK) を復元することができないようになっている。

【0034】

なお、タイトルキーファイルと各バックアップファイルの他のファイルの TKF 乱数との関連づけは、上記 (1) ~ (3) 式に限定されるものではなく、(1) ~ (3) 式以外のパターンでタイトルキーファイルとバックアップファイルの TKF 乱数と関連付けるように構成してもよい。

【0035】

ここで、乱数1～3（BN1，BN2，BN3）は、タイトルキーファイルTKF#1およびバックアップファイルTKF#2，TKF#3が記録されたセクタの図3に示したプロテクト領域に記録される。一方、TKF乱数1～3（TKFN1，TKFN2，TKFN3）はタイトルキーファイルTKF#1およびバックアップファイルTKF#2，TKF#3のユーザ領域に記録される。このため、乱数1～3（BN1，BN2，BN3）はユーザが任意の値を記録することができないが、TKF乱数1～3（TKFN1，TKFN2，TKFN3）は、例えばエディタなどの鍵管理処理を行わないアプリケーションによって任意の値が書き込まれる場合もある。このため、本実施の形態では、タイトルキーファイルTKF#1またはバックアップファイルTKF#2，TKF#3を鍵管理処理を行わない一般のアプリケーションが編集（書き込み）を行う場合には、記録部113によって乱数1～3には不当情報として「0」を書き込むようになっている。例えば、TKF#1のTKFN1に鍵管理処理を行わないアプリケーションが値を書き込む場合には、記録部113によってBN1に0が設定されることになる。TKF#2，TKF#3についても同様である。

【0036】

次に、以上のように構成された本実施の形態にかかるコンテンツ記録再生装置100によるタイトルキーファイルのバックアップ処理について説明する。まず、タイトルキーファイル（TKF）のバックアップの初期化処理について説明する。図5は、タイトルキーファイル（TKF）のバックアップの初期化処理の手順を示すフローチャートである。

【0037】

まず、ホスト部120はタイトルキー（TK）を生成する。そして、TKF初期化部141では、乱数生成部125によってTKF乱数1～3（TKFN1，TKFN2，TKFN3）を乱数生成し（ステップS501）、世代も乱数生成する（ステップS502）。

【0038】

次に、TKF初期化部141は、ドライブ部110に保持されている乱数1（BN1）を取得する（ステップS503）。乱数1の生成・取得方法は、図3で示した方法で行う。そして、乱数1（BN1）と、関連付けされているTKF乱数3（TKFN3）から生成したタイトルキーを（1）式に従って暗号化し、暗号化タイトルキー（ETK1）を生成する（ステップS504）。そして、TKF初期化部141は、乱数1（BN1）とTKF乱数1（TKFN1）と世代と生成された暗号化タイトルキー（ETK1）とからタイトルキーファイルTKF#1を生成する（ステップS505）。生成したタイトルキーファイルTKF#1は、TKF初期化部141からドライブ部110に送られて記録部113によってDVDメディア140に記録する（ステップS506）。

【0039】

次に、TKF初期化部141は、ドライブ部110に保持されている乱数2（BN2）を取得する（ステップS507）。乱数2の生成・取得方法は図3にて示した方法で行う。そして、乱数2（BN2）と、関連付けされているTKF乱数1（TKFN1）からタイトルキー（TK）を（2）式に従って暗号化し、暗号化タイトルキー（ETK2）を生成する（ステップS508）。そして、TKF初期化部141は、乱数2（BN2）とTKF乱数2（TKFN2）と世代と生成された暗号化タイトルキー（ETK2）とからバックアップファイルTKF#2を生成する（ステップS509）。生成したバックアップファイルTKF#2は、TKF初期化部141からドライブ部110に送られて記録部113によってDVDメディア140に記録する（ステップS510）。

【0040】

次に、TKF初期化部141は、ドライブ部110に保持されている乱数3（BN3）を取得する（ステップS511）。乱数3の生成・取得方法は図3にて示した方法で行う。そして、乱数3（BN3）と、関連付けされているTKF乱数2（TKFN2）からタイトルキー（TK）を（3）式に従って暗号化し、暗号化タイトルキー（ETK3）を生

成する（ステップS512）。そして、TKF初期化部141は、乱数3（BN3）とTKF乱数3（TKFN3）と世代と生成された暗号化タイトルキー（ETK3）とからバックアップファイルTKF#3を生成する（ステップS513）。生成したバックアップファイルTKF#3は、TKF初期化部141からドライブ部110に送られて記録部113によってDVDメディア140に記録する（ステップS514）。このようにしてDVDメディア140上のタイトルキーは3つのファイルに格納されることになる。

【0041】

次に、タイトルキーファイル（TKF）のバックアップの更新処理について説明する。図6-1は、タイトルキーファイル（TKF）のバックアップの更新処理の手順を示すフローチャートである。

【0042】

バックアップファイルの更新処理は、DVDメディア140のタイトルコンテンツが削除されたり追加されることにより、タイトルキー（TK）のリストが更新された場合に実行される。このとき、読み出し部112によって、DVDメディア140からタイトルキー（TKF#1）と二つのバックアップファイルTKF#2、TKF#3が読み出される。まず、タイトルキーファイル（TKF#1）と二つのバックアップファイルTKF#2、TKF#3の世代フィールドの値が全て一致するかチェックする。一致していない場合は後述する回復処理を行う。一致している場合は、以下の処理を継続する。次に、TKF更新部142は、ドライブ部110の読み出し部112からDVDメディア140上に記録された乱数1（BN1）を取得する（ステップS601）。そして、タイトルキーファイルTKF#1の暗号化タイトルキー（ETK1）を、（1）式に従って、乱数1（BN1）と、関連づけされているTKF乱数#3とによって復号化し（ステップS602）、タイトルキー（TK）を得る。そして、TKF更新部142は、TKF乱数1～3（TKFN1、TKFN2、TKFN3）を新たに乱数生成し（ステップS603）、世代を1増加して更新する（ステップS604）。

【0043】

次に、TKF更新部142はドライブ部110に乱数生成を要求して、乱数生成部111によって再生成された新たな乱数1（BN1）をドライブ部110から取得する（ステップS605）。そして、TKF更新部142は、新たな乱数1（BN1）と、関連付けされた新たなTKF乱数3（TKFN3）から、タイトルキー（TK）を（1）式に従って暗号化し、暗号化タイトルキー（ETK1）を生成する（ステップS606）。そして、TKF更新部142は、新たな乱数1（BN1）と、新たなTKF乱数1（TKFN1）と更新された世代と生成された暗号化タイトルキー（ETK1）とからタイトルキーファイルTKF#1を生成し（ステップS607）、TKF#1を更新する。更新されたタイトルキーファイルTKF#1は、TKF更新部142からドライブ部110に送られて記録部113によってDVDメディア140に記録する（ステップS608）。

【0044】

上述したステップS601からS607までの処理を、ホスト部120とドライブ110との間のデータ送受信に着目して説明する。図6-2は、タイトルキーファイルTKF#1を復号し、再生成した乱数1にて暗号化した後、TKF#1と再生成した乱数1をDVDメディア140に書き込む処理の手順を示したシーケンス図である。まず、ホスト部120からドライブ部110に乱数読み出し命令が送信される（ステップS621）。この乱数読み出し命令を受信したドライブ部110では、読み出し部112によってDVDメディア140から乱数1を読み込む（ステップS622）。そして、ドライブ部110はDVDメディア140から読み込んだ乱数1をホスト部120に送信する（ステップS623）。乱数1を受信したホスト部120ではTKF#1の復号化処理が行われる（ステップS624）。

【0045】

次いで、ホスト部120は、ドライブ部110に乱数生成命令を送信し（ステップS625）、乱数生成命令を受信したドライブ部110では乱数生成部111によって乱数1

を再生成し（ステップS626）、再生成した乱数1を一時的に蓄積しておく。ホスト部120からドライブ部110に乱数読み出し命令が送信されると（ステップS627）、ドライブ部110は一時的に蓄積された乱数1をホスト部120に送信する（ステップS628）。

【0046】

再生成された乱数1を受信したホスト部120は、再生成された乱数1を用いてTKF#1の暗号化処理を行う（ステップS629）。TKF#1の暗号化処理が終了したら、ホスト部120は、乱数書き込み命令（ETK1）をドライブ部110に送信し（ステップS630）、ドライブ部110では、この乱数書き込み命令を受信すると、記録部113によって乱数1とETK1をDVDメディア140に書き込む（ステップS630）。

【0047】

このようにTKF#1と乱数1がDVDメディア140に書き込まれると、図6-1に戻り、TKF更新部142はドライブ部110に乱数生成を要求して、乱数生成部111によって再生成された新たな乱数2（BN2）をドライブ部110から取得する（ステップS609）。そして、TKF更新部142は、新たな乱数2（BN2）と、関連付けされた新たなTKF乱数1（TKFN1）から、タイトルキー（TK）を（2）式に従って暗号化し、暗号化タイトルキー（ETK2）を生成する（ステップS610）。そして、TKF更新部142は、新たな乱数2（BN2）と、新たなTKF乱数2（TKFN2）と更新された世代と生成された暗号化タイトルキー（ETK2）とからバックアップファイルTKF#2を生成し（ステップS611）、TKF#2を更新する。更新されたバックアップファイルTKF#2は、TKF更新部142からドライブ部110に送られて記録部113によってDVDメディア140に記録する（ステップS612）。

【0048】

次に、TKF更新部142はドライブ部110に乱数生成を要求して、乱数生成部111によって再生成された新たな乱数3（BN3）をドライブ部110から取得する（ステップS613）。そして、TKF更新部142は、新たな乱数3（BN3）と、関連付けされた新たなTKF乱数2（TKFN2）からタイトルキー（TK）を（3）式に従って暗号化し、暗号化タイトルキー（ETK3）を生成する（ステップS614）。そして、TKF更新部142は、新たな乱数3（BN2）と新たなTKF乱数3（TKFN3）と更新された世代と生成された暗号化タイトルキー（ETK3）とからバックアップファイルTKF#3を生成し（ステップS615）、TKF#3を更新する。更新されたバックアップファイルTKF#3は、TKF更新部142からドライブ部110に送られて記録部113によってDVDメディア140に記録する（ステップS616）。このようにして、タイトルキーファイルTKF#1、バックアップファイルTKF#2、TKF#3は更新され、TKF#1、TKF#2、TKF#3の順にDVDメディア140に書き込まれることになる。このような順でタイトルキーファイルおよびバックアップファイルがDVDメディア140に書き込まれることにより、世代の一致か不一致かによるバックアップファイルの回復の必要性の判断を行うことができる。

【0049】

次に、タイトルキーファイル（TKF#1）およびバックアップファイル（TKF#2、TKF#3）のバックアップの回復処理について説明する。図7は、タイトルキーファイル（TKF#1）のバックアップの回復の全体処理の手順を示すフローチャートである。

【0050】

バックアップファイルの回復処理は、DVDメディア140にタイトルキーファイルTKF#1、バックアップファイルTKF#2、TKF#3のいずれか1つが存在しない場合あるいは破壊されている場合、若しくは3つのファイルTKF#1、TKF#2、TKF#3の世代が一致しない場合に実行される。具体的には、以下のような判断により行われる。

【0051】

まず、読み出し部112によって、DVDメディア140からタイトルキーファイルTKF#1およびバックアップファイルTKF#2、TKF#3が読み出され、TKF回復部143は、タイトルキーファイルTKF#1が存在しないかあるいは破壊されているかを調べる(ステップS701)。そして、タイトルキーファイルTKF#1が存在しないかあるいは破壊されている場合には(ステップS701:Yes)、バックアップファイルTKF#3による回復処理を行う(ステップS708)。

【0052】

一方、ステップS701において、タイトルキーファイルTKF#1が存在し、かつ破壊されていない場合には(ステップS701:No)、バックアップファイルTKF#2が存在しないかあるいは破壊されているかを調べる(ステップS702)。そして、バックアップファイルTKF#2が存在しないかあるいは破壊されている場合には(ステップS702:Yes)、タイトルキーファイルTKF#1による回復処理を行う(ステップS706)。

【0053】

一方、ステップS702において、バックアップファイルTKF#2が存在し、かつ破壊されていない場合には(ステップS702:No)、バックアップファイルTKF#3が存在しないかあるいは破壊されているかを調べる(ステップS703)。そして、バックアップファイルTKF#3が存在しないかあるいは破壊されている場合には(ステップS703:Yes)、バックアップファイルTKF#2による回復処理を行う(ステップS707)。

【0054】

一方、ステップS703において、バックアップファイルTKF#3が存在し、かつ破壊されていない場合には(ステップS703:No)、TKF#1の世代がTKF#2の世代(=TKF#3の世代)より大きいかな否かを調べる(ステップS704)。そして、TKF#1の世代がTKF#2の世代(=TKF#3の世代)より大きい場合には(ステップS704:Yes)、TKF#1の更新後、TKF#2の更新前にコンテンツ記録再生装置100の電源断等により更新処理が中断したものと判断して、TKF#3による回復処理を行う(ステップS708)。

【0055】

一方、ステップS704において、TKF#1の世代がTKF#2の世代(=TKF#3の世代)より大きくない場合には(ステップS704:No)、TKF#3の世代がTKF#2の世代(=TKF#1の世代)より小さいかな否かを調べる(ステップS705)。そして、TKF#3の世代がTKF#2の世代(=TKF#1の世代)より小さい場合には(ステップS704:Yes)、TKF#2の更新後、TKF#3の更新前にコンテンツ記録再生装置100の電源断等により更新処理が中断したものと判断して、TKF#2による回復処理を行う(ステップS707)。

【0056】

一方、ステップS705において、TKF#3の世代がTKF#2の世代(=TKF#1の世代)より小さくない場合には(ステップS705:No)、いずれのバックアップファイルも存在し、かつ破壊されておらず、また更新中に更新処理が中断されていないため、バックアップファイルを回復する必要なしとして、回復処理を行わずに終了する。

【0057】

次に、ステップS708におけるバックアップファイルTKF#3による回復処理について説明する。図8は、バックアップファイルTKF#3による回復処理の手順を示すフローチャートである。

【0058】

TKF回復部143は、TKF#1が存在しない場合か破壊されている場合、TKF#1の世代がTKF#2およびTKF#3の世代より大きい場合には、(3)式よりTKF#3を用いて暗号化タイトルキー(E TK3)を復号化して、タイトルキー(TK)を得て、このTKからTKF#1、TKF#2、TKF#3の回復処理を行う。

【0059】

このため、まず、TKF回復部143は、TKF#2の乱数2(BN2)が格納されるプロテクト領域に不当情報としての0が設定されているか否かを調べる(ステップS801)。そして、TKF#2の乱数2(BN2)に0が設定されている場合には(ステップS801:Yes)、例えば、エディタなどのアプリケーションによりTKF#2のユーザ領域にあるTKFN2の値が変更され、不当な更新である場合があるので、エラー処理を行って(ステップS818)、回復処理を行わずに終了する。

【0060】

一方、ステップS801において、TKF#2の乱数2(BN2)が格納されるプロテクト領域に0が設定されていない場合には(ステップS801:No)、TKF#2は正当なものであると判断して、以下の回復処理を続行する。

【0061】

TKF回復部143は、ドライブ部110からDVDメディア140上に記録された乱数3(BN3)とTKF#2、TKF#3を取得する(ステップS802)。そして、バックアップファイルTKF#3の暗号化タイトルキー(ETK3)を、乱数3(BN3)と、関連づけされているTKF乱数2(TKFN2)とによって(3)式によって復号化し(ステップS803)、タイトルキー(TK)を得る。そして、TKF更新部142は、TKF乱数1~3(TKFN1, TKFN2, TKFN3)を新たに乱数生成し(ステップS804)、世代を1増加して更新する(ステップS805)。

【0062】

次に、TKF回復部143はドライブ部110に乱数生成を要求して、乱数生成部111によって再生成された新たな乱数1(BN1)をドライブ部110から取得する(ステップS806)。そして、TKF回復部143は、新たな乱数1(BN1)と、関連付けされた新たなTKF乱数3(TKFN3)からタイトルキー(TK)を(1)式に従って暗号化し、暗号化タイトルキー(ETK1)を生成する(ステップS807)。そして、TKF回復部143は、新たな乱数1(BN1)と、新たなTKF乱数1(TKFN1)と更新された世代と生成された暗号化タイトルキー(ETK1)とからタイトルキーファイルTKF#1を生成し(ステップS808)、TKF#1を回復する。回復されたタイトルキーファイルTKF#1は、TKF回復部143からドライブ部110に送られて記録部113によって乱数1(BN1)とともにDVDメディア140に記録する(ステップS809)。

【0063】

次に、TKF回復部143はドライブ部110に乱数生成を要求して、乱数生成部111によって再生成された新たな乱数2(BN2)をドライブ部110から取得する(ステップS810)。そして、TKF回復部143は、新たな乱数2(BN2)と、関連付けされた新たなTKF乱数1(TKFN1)からタイトルキー(TK)を(2)式に従って暗号化し、暗号化タイトルキー(ETK2)を生成する(ステップS811)。そして、TKF回復部143は、新たな乱数2(BN2)と、新たなTKF乱数2(TKFN2)と更新された世代と生成された暗号化タイトルキー(ETK2)とからバックアップファイルTKF#2を生成し(ステップS812)、TKF#2を回復する。回復されたバックアップファイルTKF#2は、TKF回復部143からドライブ部110に送られて記録部113によって乱数2(BN2)とともにDVDメディア140に記録する(ステップS813)。

【0064】

次に、TKF回復部143はドライブ部110に乱数生成を要求して、乱数生成部111によって再生成された新たな乱数3(BN3)をドライブ部110から取得する(ステップS814)。そして、TKF回復部143は、新たな乱数3(BN3)と、関連付けされた新たなTKF乱数2(TKFN2)からタイトルキー(TK)を(3)式に従って暗号化し、暗号化タイトルキー(ETK3)を生成する(ステップS815)。そして、TKF回復部143は、新たな乱数3(BN3)と、新たなTKF乱数3(TKFN3)

と更新された世代と生成された暗号化タイトルキー（ETK3）とからバックアップファイルTKF#3を生成し（ステップS816）、TKF#3を回復する。回復されたバックアップファイルTKF#3は、TKF回復部143からドライブ部110に送られて記録部113によって乱数3（BN3）とともにDVDメディア140に記録する（ステップS817）。このようにして、TKF#3を用いて全てのバックアップファイルが回復されることになる。

【0065】

次に、ステップS706におけるタイトルキーファイルTKF#1による回復処理について説明する。図9は、タイトルキーファイルTKF#1による回復処理の手順を示すフローチャートである。

【0066】

TKF回復部143は、TKF#2が存在しない場合か破壊されている場合には、（1）式よりTKF#1を用いて暗号化タイトルキー（ETK1）を復号化して、タイトルキー（TK）を得て、このTKからTKF#1、TKF#2、TKF#3の回復処理を行う。

【0067】

このため、まず、TKF回復部143は、TKF#3の乱数3（BN3）に不当情報としての0が設定されているか否かを調べる（ステップS901）。そして、TKF#3の乱数3（BN3）に0が設定されている場合には（ステップS901：Yes）、例えば、エディタなどのアプリケーションによりTKF#3のユーザ領域にあるTKFN3の値が変更され、不当な更新である場合があるので、エラー処理を行って（ステップS918）、回復処理を行わずに終了する。

【0068】

一方、ステップS901において、TKF#3の乱数3（BN3）に0が設定されていない場合には（ステップS901：No）、TKF#3は正当なものであると判断して、以下の回復処理を続行する。

【0069】

TKF回復部143は、ドライブ部110からDVDメディア140上に記録された乱数1（BN1）とTKF#1、TKF#3を取得する（ステップS902）。そして、タイトルキーファイルTKF#1の暗号化タイトルキー（ETK1）を、乱数1（BN1）と、関連づけされているTKF乱数3（TKFN3）とによって（1）式によって復号化し（ステップS903）、タイトルキー（TK）を得る。そして、TKF更新部142は、TKF乱数1～3（TKFN1、TKFN2、TKFN3）を新たに乱数生成し（ステップS904）、世代を1増加して更新する（ステップS905）。

【0070】

これ以降のステップS906からS917までのTKF#1、TKF#2、TKF#3の回復処理は、図8のステップS906からS917までの処理と同様に行われる。このようにして、TKF#1を用いて全てのバックアップファイルが回復されることになる。

【0071】

次に、ステップS707におけるバックアップファイルTKF#2による回復処理について説明する。図10は、バックアップファイルTKF#2による回復処理の手順を示すフローチャートである。

【0072】

TKF回復部143は、TKF#3が存在しない場合か破壊されている場合、TKF#3の世代がTKF#2およびTKF#1の世代より小さい場合には、（2）式よりTKF#2を用いて暗号化タイトルキー（ETK2）を復号化して、タイトルキーファイル（TKF）を得て、このTKFからTKF#1、TKF#2、TKF#3の回復処理を行う。

【0073】

このため、まず、TKF回復部143は、TKF#1の乱数1（BN1）に不当情報としての0が設定されているか否かを調べる（ステップS1001）。そして、TKF#1

の乱数1 (BN1) に0が設定されている場合には (ステップS1001: Yes)、例えば、エディタなどのアプリケーションによりTKF#1のユーザ領域にあるTKFN1の値が変更され、不当な更新である場合があるので、エラー処理を行って (ステップS1018)、回復処理を行わずに終了する。

【0074】

一方、ステップS1001において、TKF#1の乱数1 (BN1) に0が設定されていない場合には (ステップS1001: No)、TKF#1は正当なものであると判断して、以下の回復処理を続行する。

【0075】

TKF回復部143は、ドライブ部110からDVDメディア140上に記録された乱数2 (BN2) とTKF#2、TKF#1を取得する (ステップS1002)。そして、バックアップファイルTKF#2の暗号化タイトルキー (ETK2) を、乱数2 (BN2) と、関連づけされているTKF乱数1 (TKFN1) とによって (2) 式によって復号化し (ステップS1003)、タイトルキー (TK) を得る。そして、TKF更新部142は、TKF乱数1~3 (TKFN1, TKFN2, TKFN3) を新たに乱数生成し (ステップS1004)、世代を1増加して更新する (ステップS1005)。

【0076】

これ以降のステップS1006からS1017までのTKF#1、TKF#2、TKF#3の回復処理は、図8のステップS906からS917までの処理と同様に行われる。このようにして、TKF#2を用いて全てのバックアップファイルが回復されることになる。

【0077】

このように実施の形態1では、タイトルキー (TK) の暗号化ファイルを3つ用意し、それぞれの暗号化タイトルキーを、自己の乱数と自己に関連付けられた他のファイルのTKF乱数によって (1) ~ (3) 式のように暗号化している。このため、例えば、攻撃者が予め1つのバックアップファイルを他のメディアにコピーしておき、正規の手順でタイトルコンテンツの一部を他のメディアに移動して、タイトルキーファイルが更新され、攻撃者がタイトルキーファイルをDVDメディアから削除し、当該DVDメディアに他のメディアにコピーしておいたバックアップファイルを復元したとしても、少なくとも2つのファイルがなければ、(1) ~ (3) 式よりタイトルキーを復号化できず、また他の2つのファイルは更新処理によって更新されているので、結局タイトルキーを復元することができない。このため、DVDメディアから削除したタイトルコンテンツに対するタイトルキーを不正に復元されてしまうことを防止し、タイトルコンテンツの不正な利用を防止することができる。

【0078】

また、例えば、攻撃者が予め1つのバックアップファイルをリネームして同一のDVDメディアに保存した場合でも、タイトルキーファイルを作成するアプリケーションではないアプリケーションが、タイトルキーファイルを編集した場合、プロテクト領域に記録される乱数1~3に不当情報である0が設定されてしまうので、バックアップファイルの不当な回復処理が実行されず、結局タイトルキーを復元することができない。このため、タイトルコンテンツの不正な利用を防止することができる。

【0079】

(変形例)

実施の形態1では、タイトルキーファイルTKF#1およびバックアップファイルTKF#2、TKF#3の世代は、初期化時に乱数生成し、タイトルコンテンツが削除されたり追加されたりするなどによりタイトルキーのリストが変化するたびに、更新処理の一貫として世代を1ずつ更新するように構成されていた。しかし、世代を、初期化時に限らず更新処理に毎回乱数生成するように構成してもよい。図11は、世代を更新処理時に毎回乱数生成した場合におけるタイトルキーファイル (TKF) のバックアップの回復処理の全体処理の手順を示すフローチャートである。

【0080】

かかるバックアップ回復の全体処理では、ステップS1104とS1105のみが図7で説明した全体処理と異なっている。すなわち、ステップS1104では、TKF#2とTKF#3の世代の値は一致するが、TKF#2およびTKF#3の世代の値がTKF#1の世代の値と一致しないかどうかを判断している。また、ステップS1105では、TKF#1とTKF#2の世代の値は一致するが、TKF#1およびTKF#2の世代の値とTKF#3の世代の値とは一致しないかどうかを判断している。これは、本変形例では、更新処理ごとに毎回、世代を乱数生成しているためである。

【0081】

(実施の形態2)

実施の形態1では、タイトルキーファイルTKF#1、バックアップファイルTKF#2、TKF#3の構造が図4-1に示すように同一であったが、この実施の形態2では、バックアップファイルTKF#3の構造がタイトルキーファイルTKF#1およびバックアップファイルTKF#2と異なっている。

【0082】

実施の形態2にかかる記録再生装置の構成は、図1で説明した実施の形態1の記録再生装置と同様である。

【0083】

図12は、実施の形態2のタイトルキーファイルとバックアップファイルの構造を示す説明図である。本実施の形態では、バックアップファイルTKF#3が暗号化タイトルキーとTKF乱数3を有さず、その代わりに、TKF乱数1(TKFN1)とTKF乱数2(TKFN2)を備えている点、およびタイトルキーファイルTKF#1の暗号化タイトルキー(ETK1)とバックアップファイルTKF#2の暗号化タイトルキー(ETK2)の計算方式が実施の形態1と異なっている。

【0084】

タイトルキーファイルTKF#1とバックアップファイルTKF#2は、実施の形態1のTKF#1、TKF#2と同様に、乱数1, 2(BN1, BN2)と、世代と、TKF乱数1, 2(TKFN1, TKFN2)と暗号化タイトルキー(ETK1, ETK2)から構成されている。TKF#1のTKF乱数1(TKFN1)は、TKF#1自身以外のバックアップファイルTKF#2の暗号化タイトルキー(ETK2)を生成するための乱数である。TKF#2のTKF乱数2(TKFN2)は、TKF#2自身以外のTKF#1の暗号化タイトルキー(ETK1)を生成するための乱数である。

【0085】

バックアップファイルTKF#3は、TKF#1およびTKF#2の構造と異なり、乱数3(BN3)と、世代と、TKF乱数1(TKFN1)と、TKF乱数2(TKFN2)とを有している。このTKF#3のTKF乱数のうち、TKFN1は、タイトルキーファイルTKF#1のTKF乱数1(TKFN1)と同じ値が記録され、TKFN2は、バックアップファイルTKF#2のTKF乱数2(TKFN2)と同じ値が記録される。

【0086】

暗号化タイトルキー(ETK1, ETK2)は、タイトルキーファイルTKF#1またはバックアップファイルTKF#2、TKF#3に登録されている乱数(BN1, BN2)と、関連づけられている他のファイルに登録されているTKF乱数(TKFN1, TKFN2)によって、タイトルキーファイルの全タイトルキーを暗号化したデータである。暗号化タイトルキー(ETK1, ETK2)は、次の(4)、(5)式で示される。

【0087】

$$ETK1 = I(TK, BN1, TKFN2) \quad \dots (4)$$

$$ETK2 = I(TK, BN2, TKFN1) \quad \dots (5)$$

ここで、TKはタイトルキーを示し、Iは、第1パラメタ(TK)に第2パラメタ(BN1, 2)と第3パラメタ(TKFN1, 2)を暗号鍵として暗号処理を施すことを示している。暗号処理Iには、たとえばAES(Advanced Encryption Standard)などのよく

知られた暗号アルゴリズムを用いればよい。

【0088】

次に、以上のように構成された本実施の形態にかかるコンテンツ記録再生装置100によるタイトルキーファイルのバックアップ処理について説明する。

【0089】

まず、タイトルキーファイル(TKF)のバックアップの初期化处理について説明する。図13は、タイトルキーファイル(TKF)のバックアップの初期化处理の手順を示すフローチャートである。本実施の形態のバックアップ初期化处理では、バックアップファイルTKF#3の構造が図12に示すとおりTKF#1、TKF#2と異なり、また暗号化タイトルキー(ETK1、ETK2)が(4)、(5)式で求められることから、タイトルキーファイルTKF#1の暗号化タイトルキー(ETK1)の生成処理と、タイトルキーファイルTKF#1の生成処理と、バックアップファイルTKF#3の生成処理が図5で説明した実施の形態1のバックアップ初期化处理と異なっている。

【0090】

まず、ホスト部120はタイトルキー(TK)を生成する。そして、TKF初期化部141は、乱数生成部125によってTKF乱数1、2(TKF N1、TKF N2)を乱数生成し(ステップS1301)、世代も乱数生成する(ステップS1302)。

【0091】

次に、TKF初期化部141は、ドライブ部110で保持されている乱数1(BN1)を取得する(ステップS503)。ここで乱数1の生成・取得方法は、図3で示した方法で行う。そして、乱数1(BN1)と、関連付けされているTKF乱数2(TKF N2)から、生成したタイトルキーを(4)式に従って暗号化し、暗号化タイトルキー(ETK1)を生成する(ステップS1304)。そして、TKF初期化部141は、乱数1(BN1)とTKF乱数1(TKF N1)と世代と生成された暗号化タイトルキー(ETK1)とからタイトルキーファイルTKF#1を生成する(ステップS1305)。生成したタイトルキーファイルTKF#1は、TKF初期化部141からドライブ部110に送られて記録部113によってDVDメディア140に記録する(ステップS1306)。

【0092】

次に、TKF初期化部141は、ドライブ部110で保持されている乱数2(BN2)を取得する(ステップS507)。ここで、乱数2の生成・取得方法は図3にて示した方法で行う。そして、乱数2(BN2)と、関連付けされているTKF乱数1(TKF N1)からタイトルキー(TK)を(5)式に従って暗号化し、暗号化タイトルキー(ETK2)を生成する(ステップS1308)。そして、TKF初期化部141は、乱数2(BN2)とTKF乱数2(TKF N2)と世代と生成された暗号化タイトルキー(ETK2)とからバックアップファイルTKF#2を生成する(ステップS1309)。生成したバックアップファイルTKF#2は、TKF初期化部141からドライブ部110に送られて記録部113によってDVDメディア140に記録する(ステップS1310)。

【0093】

次に、TKF初期化部141は、ドライブ部110で保持されている乱数3(BN3)を取得する(ステップS1311)。乱数3の生成・取得方法は図3にて示した方法で行う。そして、乱数3(BN3)とTKF乱数1(TKF N1)とTKF乱数2(TKF N2)と世代とから図12に示す構造のバックアップファイルTKF#3を生成する(ステップS1312)。生成したバックアップファイルTKF#3は、TKF初期化部141からドライブ部110に送られて記録部113によってDVDメディア140に記録する(ステップS1313)。以上のような処理で、図12に示すタイトルキーファイルTKF#1、バックアップファイルTKF#2、TKF#3が生成される。

【0094】

次に、タイトルキーファイル(TKF)のバックアップの更新処理について説明する。図14は、実施の形態2におけるタイトルキーファイル(TKF)のバックアップの更新処理の手順を示すフローチャートである。本実施の形態では、バックアップファイルTK

F#3の構造が図12に示すとおりTKF#1、TKF#2と異なり、また暗号化タイトルキー（ETK1、ETK2）が（4）、（5）式で求められることからタイトルキーファイル（TKF#1）の復号化処理、タイトルキーファイルTKF#1の暗号化タイトルキー（ETK1）の生成処理、タイトルキーファイルTKF#1の生成処理、バックアップファイルTKF#3の生成処理が図6-1で説明した実施の形態1の更新処理と異なっている。

【0095】

本実施の形態でもバックアップファイルの更新処理は、DVDメディア140のタイトルコンテンツが削除されたり追加されることにより、タイトルキー（TK）のリストが更新された場合に実行される。このとき、読み出し部112によって、DVDメディア140からタイトルキー（TKF#1）と二つのバックアップファイルTKF#2、TKF#3が読み出される。まず、TKF更新部142は、ドライブ部110の読み出し部112からDVDメディア140上に記録された乱数1（BN1）を取得する（ステップS1401）。そして、タイトルキーファイルTKF#1の暗号化タイトルキー（ETK1）を、（4）式に従って、乱数1（BN1）と関連づけされているTKF乱数#2とによって復号化し（ステップS1402）、タイトルキー（TK）を得る。そして、TKF更新部142は、TKF乱数1（TKFN1）およびTKF乱数2（TKFN2）を新たに乱数生成し（ステップS1403）、世代を1増加して更新する（ステップS1404）。

【0096】

次に、TKF更新部142は、ドライブ部110に乱数生成を要求して、乱数生成部111によって再生成された新たな乱数1（BN1）をドライブ部110から取得する（ステップS1405）。そして、TKF更新部142は、新たな乱数1（BN1）と、関連付けされた新たなTKF乱数2（TKFN2）から、タイトルキー（TK）を（4）式に従って暗号化し、暗号化タイトルキー（ETK1）を生成する（ステップS1406）。そして、TKF更新部142は、新たな乱数1（BN1）と、新たなTKF乱数1（TKFN1）と更新された世代と生成された暗号化タイトルキー（ETK1）とからタイトルキーファイルTKF#1を生成し（ステップS1407）、TKF#1を更新する。更新されたタイトルキーファイルTKF#1は、TKF更新部142からドライブ部110に送られて記録部113によってDVDメディア140に記録する（ステップS1408）。

【0097】

次に、TKF更新部142はドライブ部110に乱数生成を要求して、乱数生成部111によって再生成された新たな乱数2（BN2）をドライブ部110から取得する（ステップS1409）。そして、TKF更新部142は、新たな乱数2（BN2）と、関連付けされた新たなTKF乱数1（TKFN1）から、タイトルキー（TK）を（5）式に従って暗号化し、暗号化タイトルキー（ETK2）を生成する（ステップS1410）。そして、TKF更新部142は、新たな乱数2（BN2）と、新たなTKF乱数2（TKFN2）と更新された世代と生成された暗号化タイトルキー（ETK2）とからバックアップファイルTKF#2を生成し（ステップS1411）、TKF#2を更新する。更新されたバックアップファイルTKF#2は、TKF更新部142からドライブ部110に送られて記録部113によってDVDメディア140に記録する（ステップS1412）。

【0098】

次に、TKF更新部142は、ドライブ部110に乱数生成を要求して、乱数生成部111によって再生成された新たな乱数3（BN3）をドライブ部110から取得する（ステップS1413）。そして、TKF更新部142は、新たな乱数3（BN3）と、更新された世代と、新たなTKF乱数1（TKFN1）と、新たなTKF乱数2（TKFN2）とから、図12に示す構造のバックアップファイルTKF#3を生成し（ステップS1414）、TKF#3を更新する。更新されたバックアップファイルTKF#3は、TKF更新部142からドライブ部110に送られて記録部113によってDVDメディア140に記録する（ステップS1415）。このようにして、タイトルキーファイルTKF

1、バックアップファイルTKF# 2、TKF# 3は更新され、TKF# 1、TKF# 2、TKF# 3の順にDVDメディア140に書き込まれることになる。

【0099】

次に、タイトルキーファイル(TKF# 1)およびバックアップファイル(TKF# 2、TKF# 3)のバックアップの回復処理について説明する。図15は、タイトルキーファイル(TKF# 1)のバックアップの回復の全体処理の手順を示すフローチャートである。本実施の形態では、バックアップファイルTKF# 3の構造が図12に示すとおりTKF# 1、TKF# 2と異なり、また暗号化タイトルキー(ETK1、ETK2)が(4)、(5)式で求められることから、各回復処理において用いるファイルが実施の形態1の回復処理と異なっている。

【0100】

すなわち、ステップS1501からS1505までの判断処理は、図7で説明したステップS701からS705までの処理と同様に行われる。本実施の形態では、ステップS1502でTKF# 2が存在しない場合あるいは破壊されている場合には、TKF# 1、TKF# 3を用いた回復処理が行われる(ステップS1506)。また、ステップS1503でTKF# 3が存在しない場合あるいは破壊されている場合、ステップS1505でTKF# 3の世代がTKF# 1およびTKF# 2の世代より小さい場合には、TKF# 1、TKF# 2を用いた回復処理が行われる(ステップS1507)。さらに、ステップS1501でTKF# 1が存在しない場合あるいは破壊されている場合、またはステップS1504でTKF# 1の世代がTKF# 2およびTKF# 3の世代より大きい場合、TKF# 2、TKF# 3を用いた回復処理が行われる(ステップS1508)。

【0101】

次に、ステップS1508におけるバックアップファイルTKF# 2の暗号化タイトルキー(ETK2)を復号することによる回復処理について説明する。図16は、バックアップファイルTKF# 2、# 3による回復処理の手順を示すフローチャートである。本実施の形態では、バックアップファイルTKF# 2を用いてバックアップファイルTKF# 3の乱数3が不当情報(「0」)として設定されているか否かを調べている点、バックアップファイルTKF# 2の暗号化タイトルキー(ETK2)の復号処理、タイトルキーファイルTKF# 1の暗号化タイトルキー(ETK1)の生成処理、タイトルキーファイルTKF# 1の生成処理、バックアップファイルTKF# 3の生成処理が、図8で説明した実施の形態1のTKF# 3による回復処理と異なっている。

【0102】

まず、TKF回復部143は、TKF# 3の乱数3(BN3)が格納されるプロテクト領域に不当情報としての0が設定されているか否かを調べる(ステップS1601)。そして、TKF# 3の乱数3(BN3)に0が設定されている場合には(ステップS1601: Yes)、例えば、エディタなどのアプリケーションによりTKF# 3のユーザ領域にあるTKFN1、TKFN2の値が変更され、不当な更新である場合があるので、エラー処理を行って(ステップS1617)、回復処理を行わずに終了する。

【0103】

一方、ステップS1601において、TKF# 3の乱数3(BN3)が格納されるプロテクト領域に0が設定されていない場合には(ステップS1601: No)、TKF# 3は正当なものであると判断して、以下の回復処理を続行する。

【0104】

TKF回復部143は、ドライブ部110からDVDメディア140上に記録された乱数2(BN2)とTKF# 2、TKF# 3を取得する(ステップS1602)。そして、バックアップファイルTKF# 2の暗号化タイトルキー(ETK2)を、乱数2(BN2)と、TKF# 3に格納されているTKF乱数1(TKFN1)とによって(5)式によって復号化し(ステップS1603)、タイトルキー(TK)を得る。そして、TKF更新部142は、TKF乱数1、2(TKFN1、TKFN2)を新たに乱数生成し(ステップS1604)、世代を1増加して更新する(ステップS1605)。

【0105】

次に、TKF回復部143はドライブ部110に乱数生成を要求して、乱数生成部111によって再生成された新たな乱数1 (BN1) をドライブ部110から取得する (ステップS1606)。そして、TKF回復部143は、新たな乱数1 (BN1) と、関連付けられた新たなTKF乱数2 (TKFN2) からタイトルキー (TK) を (4) 式に従って暗号化し、暗号化タイトルキー (ETK1) を生成する (ステップS1607)。そして、TKF回復部143は、新たな乱数1 (BN1) と、新たなTKF乱数1 (TKFN1) と更新された世代と生成された暗号化タイトルキー (ETK1) とからタイトルキーファイルTKF#1を生成し (ステップS1608)、TKF#1を回復する。回復されたタイトルキーファイルTKF#1は、TKF回復部143からドライブ部110に送られて乱数1 (BN1) とともに記録部113によってDVDメディア140に記録する (ステップS1609)。

【0106】

次に、TKF回復部143はドライブ部110に乱数生成を要求して、乱数生成部111によって再生成された新たな乱数2 (BN2) をドライブ部110から取得する (ステップS1610)。そして、TKF回復部143は、新たな乱数2 (BN2) と、関連付けられた新たなTKF乱数1 (TKFN1) からタイトルキー (TK) を (5) 式に従って暗号化し、暗号化タイトルキー (ETK2) を生成する (ステップS1611)。そして、TKF回復部143は、新たな乱数2 (BN2) と、新たなTKF乱数2 (TKFN2) と更新された世代と生成された暗号化タイトルキー (ETK2) とからバックアップファイルTKF#2を生成し (ステップS1612)、TKF#2を回復する。回復されたバックアップファイルTKF#2は、TKF回復部143からドライブ部110に送られて記録部113によって乱数2 (BN2) とともにDVDメディア140に記録する (ステップS1613)。

【0107】

次に、TKF回復部143はドライブ部110に乱数生成を要求して、乱数生成部111によって再生成された新たな乱数3 (BN3) をドライブ部110から取得する (ステップS1614)。そして、TKF回復部143は、新たな乱数3 (BN3) と、新たなTKF乱数1 (TKFN1) と、新たなTKF乱数2 (TKFN2) と、更新された世代とから、図12に示す構造のバックアップファイルTKF#3を生成し (ステップS1615)、TKF#3を回復する。回復されたバックアップファイルTKF#3は、TKF回復部143からドライブ部110に送られて記録部113によって乱数3 (BN3) とともにDVDメディア140に記録する (ステップS1616)。このようにして、TKF#2およびTKF#3を用いて全てのバックアップファイルが回復されることになる。

【0108】

次に、タイトルキーファイルTKF#1およびバックアップファイルTKF#3の回復処理について説明する。図17は、タイトルキーファイルTKF#1、バックアップファイル#3による回復処理の手順を示すフローチャートである。本実施の形態では、バックアップファイルTKF#1の暗号化タイトルキー (ETK1) の復号処理、タイトルキーファイルTKF#1の暗号化タイトルキー (ETK1) の生成処理、タイトルキーファイルTKF#1の生成処理、バックアップファイルTKF#3の生成処理が、図9で説明した実施の形態1におけるTKF#1による回復処理と異なっている。

【0109】

まず、TKF回復部143は、TKF#3の乱数3 (BN3) が格納されるプロテクト領域に不当情報としての0が設定されているか否かを調べる (ステップS1601)。そして、TKF#3の乱数3 (BN3) に0が設定されている場合には (ステップS1701: Yes)、例えば、エディタなどのアプリケーションによりTKF#3のユーザ領域にあるTKFN1、TKFN2の値が変更され、不当な更新である場合があるので、エラー処理を行って (ステップS1717)、回復処理を行わずに終了する。

【0110】

一方、ステップS1701において、TKF#3の乱数3(BN3)が格納されるプロテクト領域に0が設定されていない場合には(ステップS1701:No)、TKF#3は正当なものであると判断して、以下の回復処理を続行する。

【0111】

TKF回復部143は、ドライブ部110からDVDメディア140上に記録された乱数1(BN1)とTKF#1、TKF#3を取得する(ステップS1702)。そして、バックアップファイルTKF#1の暗号化タイトルキー(ETK1)を、乱数1(BN1)と、TKF#3に格納されているTKF乱数2(TKFN2)とによって(4)式によって復号化し(ステップS1703)、タイトルキー(TK)を得る。そして、TKF更新部142は、TKF乱数1、2(TKFN1、TKFN2)を新たに乱数生成し(ステップS1704)、世代を1増加して更新する(ステップS1705)。

【0112】

これ以降のステップS1706からS1716までのTKF#1、TKF#2、TKF#3の回復処理は、図16のステップS1606からS1616までの処理と同様に行われる。このようにして、TKF#1およびTKF#3を用いて全てのバックアップファイルが回復されることになる。

【0113】

次に、タイトルキーファイルTKF#1、バックアップファイル#2による回復処理について説明する。図18は、タイトルキーファイルTKF#1、バックアップファイルTKF#2による回復処理の手順を示すフローチャートである。TKF回復部143は、TKF#3が存在しない場合か破壊されている場合、もしくはTKF#3の世代がTKF#2およびTKF#1の世代より小さい場合には、TKF#1およびTKF#2を用いてTKF#3の回復処理を行う。

【0114】

このため、まず、TKF回復部143は、TKF#1の乱数1(BN1)およびTKF#2の乱数2(BN2)に不当情報としての0が設定されているか否かを調べる(ステップS1801)。そして、TKF#1の乱数1(BN1)およびTKF#2の乱数2(BN2)に0が設定されている場合には(ステップS1801:Yes)、例えば、エディタなどのアプリケーションによりタイトルキーファイルTKF#1のユーザ領域にあるTKFN2またはバックアップファイルTKF#2のユーザ領域にあるTKFN1の値が変更され、不当な更新である場合があるので、エラー処理を行って(ステップS1805)、回復処理を行わずに終了する。

【0115】

一方、ステップS1801において、TKF#1の乱数1(BN1)およびTKF#2の乱数2(BN2)に0が設定されていない場合には(ステップS1801:No)、TKFは正当なものであると判断して、以下の回復処理を続行する。

【0116】

TKF回復部143は、ドライブ部110からメディア上に記録された乱数(BN3)とTKF#1、TKF#2を取得する(ステップS1802)。そしてTKF#1からTKF乱数1(TKFN1)と世代を、TKF#2からTKF乱数2(TKFN2)と世代を読み出し、新たな乱数3(BN3)と世代とTKF乱数1(TKFN1)とTKF乱数2(TKFN2)とから、図12に示す構造のバックアップファイルTKF#3を生成し(ステップS1803)、TKF#3を回復する。回復されたバックアップファイルTKF#3は、TKF回復部143からドライブ部110に送られて記録部113によって乱数3(BN3)とともにDVDメディア140に記録する(ステップS1804)。このようにして、TKF#1、TKF#2を用いてTKF#3のバックアップファイルが回復されることになる。

【0117】

このように、実施の形態2にでは、タイトルキー(TK)の暗号化ファイルをTKF#1、TKF#2の2つ用意し、TKF#3を乱数3とTKF乱数2とTKF乱数3と世代

とで構成し、TKF#1、TKF#2の暗号化タイトルキーを、自己の乱数と互いのTKF乱数によって(4)、(5)のように暗号化している。このため、実施の形態1と同様に、DVDメディアから削除したタイトルコンテンツに対するタイトルキーを不正に復元されてしまうことを防止し、タイトルコンテンツの不正な利用を防止することができる。

【0118】

(変形例2)

上述した実施の形態1および2のコンテンツ記録再生装置100において、ドライブ部110とホスト部120がバス30にて接続された構成について説明してきたが、ドライブ部110とホスト部120が内部バスで接続され、一体で構成することもできる。図19は、ドライブ部110とホスト部120が内部バス1930で接続され、一体構成されたコンテンツ記録再生装置1900の構成を示すブロック図である。

【0119】

図19に示すように、ドライブ部110に含まれる各部は、実施の形態と同様のであるが、ホスト部1920では、乱数生成部を備えていない。図19の構成では、ドライブ部110内の乱数生成部111が、ホスト部1920およびドライブ部110から共用で利用されるようになっている。

【0120】

なお、図19では乱数生成部111がドライブ部110に含まれる構成を採用しているが、この他、ドライブ部110には乱数生成部が含まれず、ホスト部1920にのみ備えたり、ドライブ部110とホスト部1920には直接含まれず、装置内の別の処理部に備えるように構成してもよい。

【0121】

なお、実施の形態1および2のコンテンツ記録再生装置で実行されるコンテンツ記録再生プログラムは、ROM等に予め組み込まれて提供される。

【0122】

実施の形態1および2のコンテンツ記録再生装置で実行されるコンテンツ記録再生プログラムは、インストール可能な形式又は実行可能な形式のファイルでCD-ROM、フレキシブルディスク(FD)、CD-R、DVD等のコンピュータで読み取り可能な記録媒体に記録して提供するように構成してもよい。

【0123】

さらに、実施の形態1および2のコンテンツ記録再生装置で実行されるコンテンツ記録再生プログラムを、インターネット等のネットワークに接続されたコンピュータ上に格納し、ネットワーク経由でダウンロードさせることにより提供するように構成しても良い。また、実施の形態1および2のコンテンツ記録再生装置で実行されるコンテンツ記録再生プログラムをインターネット等のネットワーク経由で提供または配布するように構成しても良い。

【0124】

実施の形態1および2のコンテンツ記録再生装置で実行されるコンテンツ記録再生プログラムは、上述した各部(コンテンツ暗号化処理部121、コンテンツ復号化処理部122、TKF暗号化処理部123、バックアップ処理部140)を含むモジュール構成となっており、実際のハードウェアとしてはCPU(プロセッサ)が上記ROMからコンテンツ記録再生プログラムを読み出して実行することにより上記各部が主記憶装置上にロードされ、コンテンツ暗号化処理部121、コンテンツ復号化処理部122、TKF暗号化処理部123、バックアップ処理部140が主記憶装置上に生成されるようになっている。

【0125】

なお、実施の形態1および2のコンテンツ記録再生装置は、DVDレコーダのような組み込み機器ではなく、CPUなどの制御装置と、ROM(Read Only Memory)やRAMなどの記憶装置と、HDD、CDドライブ装置などの外部記憶装置と、ディスプレイ装置などの表示装置と、キーボードやマウスなどの入力装置を備えており、通常のコンピュータを利用した構成とすることもできる。この場合に、ホスト部120とドライブ部110と

を繋ぐバスは、例えば、USB等を利用することができる。

【0126】

なお、本発明は、上記実施の形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化することができる。

【図面の簡単な説明】

【0127】

【図1】実施の形態1にかかるコンテンツ記録再生装置100の構成を示すブロック図である。

【図2】セクタの構造を示す説明図である。

【図3】乱数をDVDメディア140に書き込む処理の手順を示すシーケンス図である。

【図4-1】実施の形態1のタイトルキーファイルとバックアップファイルの構造を示す説明図である。

【図4-2】暗号化キーファイルのデータ構造を示す説明図である。

【図5】タイトルキーファイル(TKF)のバックアップの初期化処理の手順を示すフローチャートである。

【図6-1】タイトルキーファイル(TKF)のバックアップの更新処理の手順を示すフローチャートである。

【図6-2】タイトルキーファイルTKF#1を復号し、再生成した乱数1にて暗号化した後、TKF#1と再生成した乱数1をDVDメディア140に書き込む処理の手順を示したシーケンス図である。

【図7】タイトルキーファイル(TKF)のバックアップの回復の全体処理の手順を示すフローチャートである。

【図8】バックアップファイルTKF#3による回復処理の手順を示すフローチャートである。

【図9】バックアップファイルTKF#1による回復処理の手順を示すフローチャートである。

【図10】バックアップファイルTKF#2による回復処理の手順を示すフローチャートである。

【図11】世代を更新処理時に毎回乱数生成した場合におけるタイトルキーファイル(TKF)のバックアップの回復処理の全体処理の手順を示すフローチャートである。

【図12】実施の形態2のタイトルキーファイルとバックアップファイルの構造を示す説明図である。

【図13】タイトルキーファイル(TKF)のバックアップの初期化処理の手順を示すフローチャートである。

【図14】実施の形態2におけるタイトルキーファイル(TKF)のバックアップの更新処理の手順を示すフローチャートである。

【図15】実施の形態2におけるタイトルキーファイル(TKF#1)のバックアップの回復の全体処理の手順を示すフローチャートである。

【図16】実施の形態2におけるバックアップファイルTKF#2、#3による回復処理の手順を示すフローチャートである。

【図17】実施の形態2におけるタイトルキーファイルTKF#1、バックアップファイル#3による回復処理の手順を示すフローチャートである。

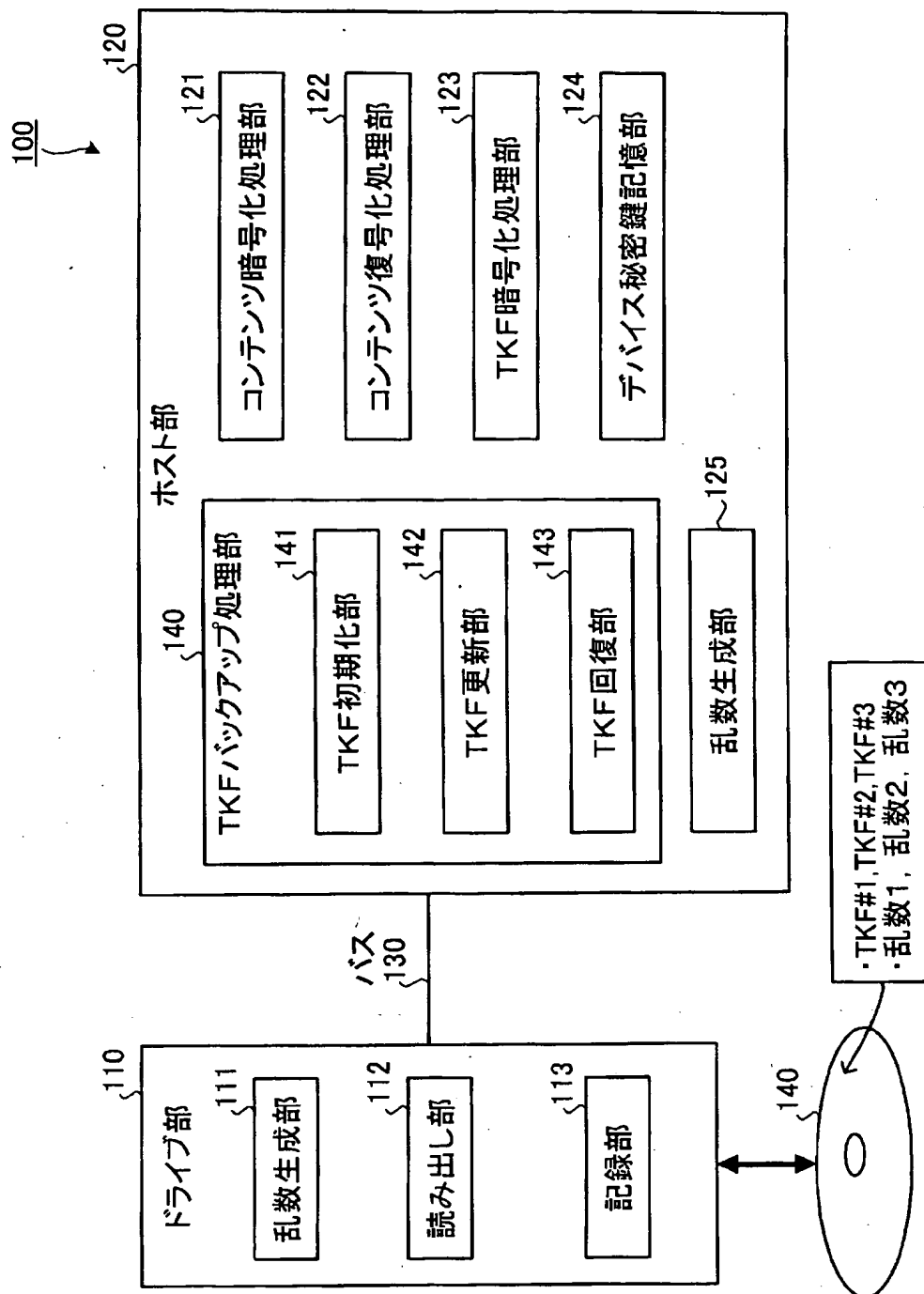
【図18】実施の形態2におけるタイトルキーファイルTKF#1、バックアップファイルTKF#2による回復処理の手順を示すフローチャートである。

【図19】ドライブ部110とホスト部120が内部バスで接続され、一体構成されたコンテンツ記録再生装置1900の構成を示すブロック図である。

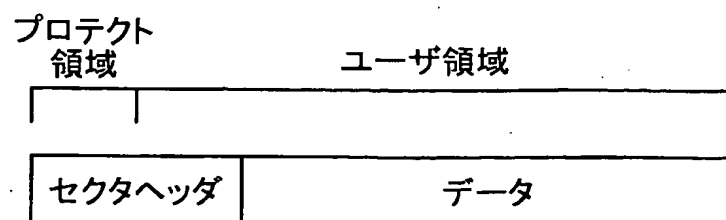
【符号の説明】

【0128】

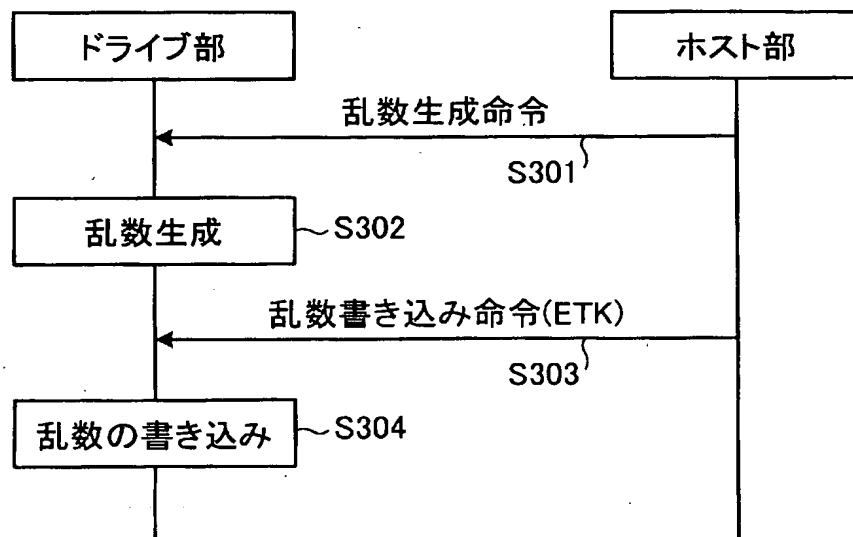
1 0 0	コンテンツ記録再生装置
1 1 0	ドライブ部
1 1 1	乱数生成部
1 1 2	読み出し部
1 1 3	記録部
1 2 0	ホスト部
1 2 1	コンテンツ暗号化処理部
1 2 2	コンテンツ復号化処理部
1 2 3	TKF 暗号化処理部
1 2 4	デバイス秘密鍵記憶部
1 2 5	乱数生成部
1 3 0	バス
1 4 0	D V D メディア



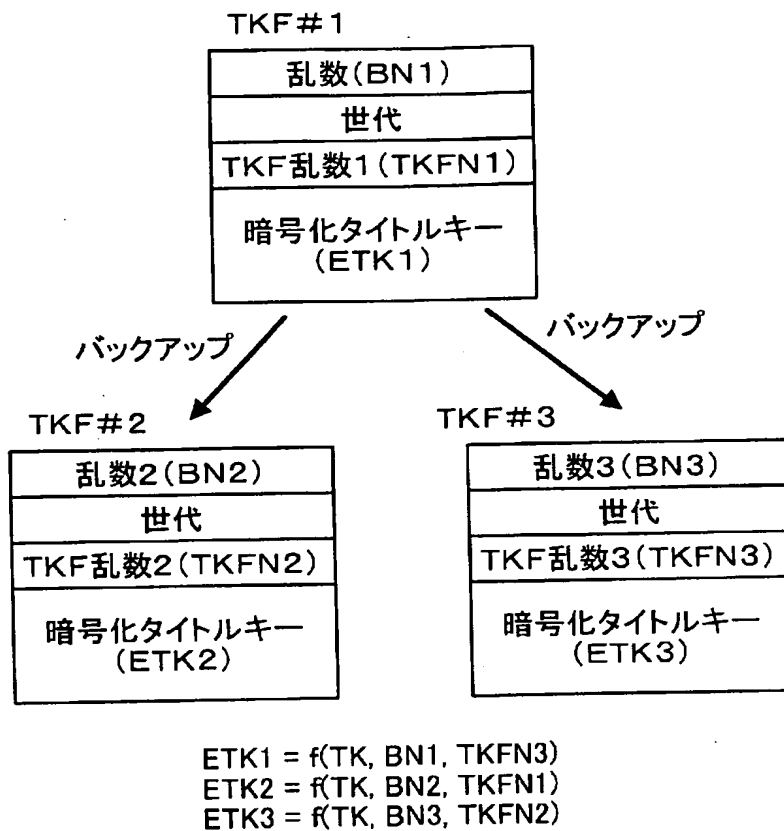
【図 2】



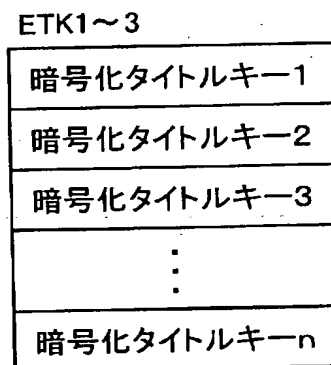
【図 3】



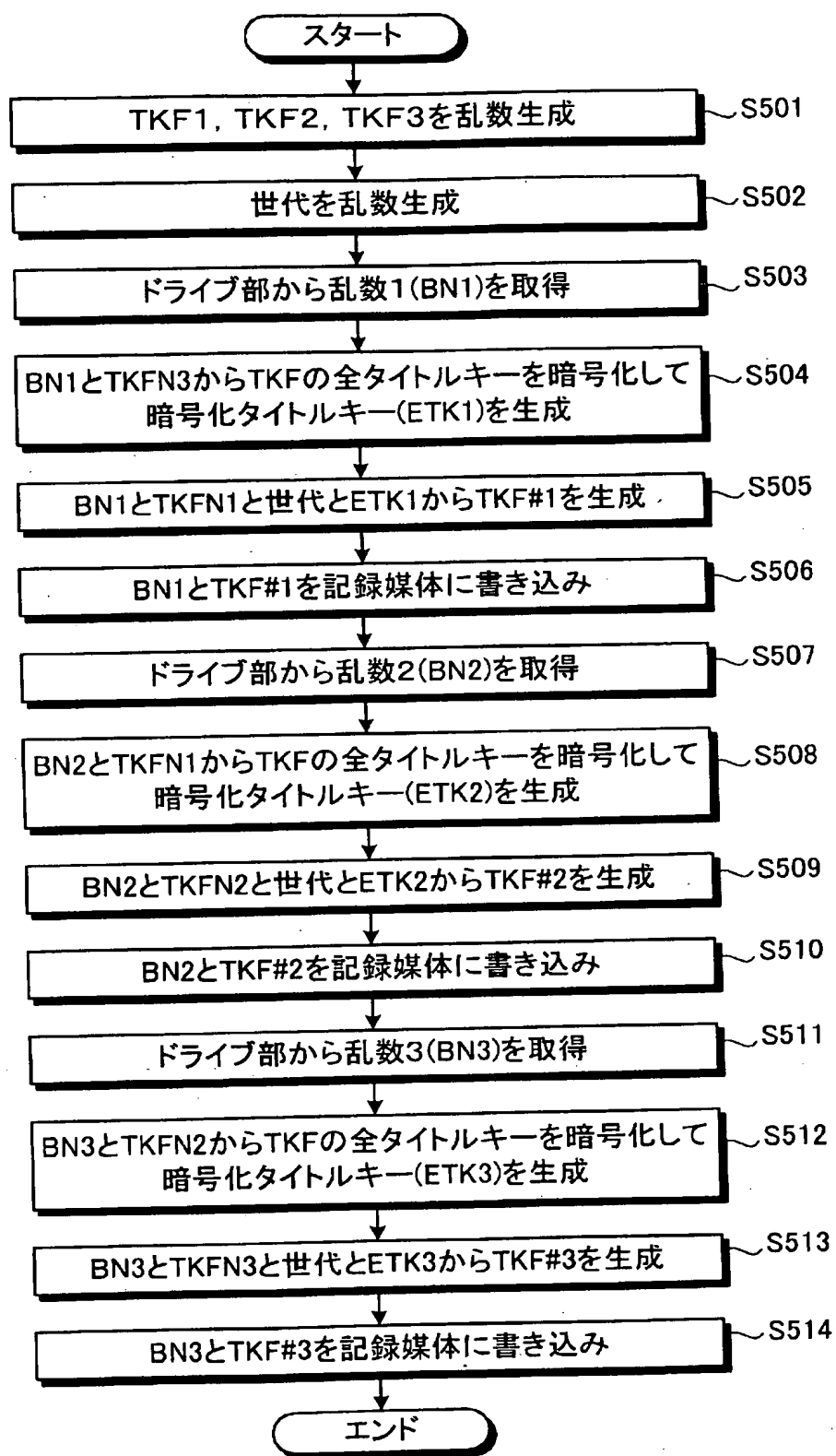
【図 4 - 1】



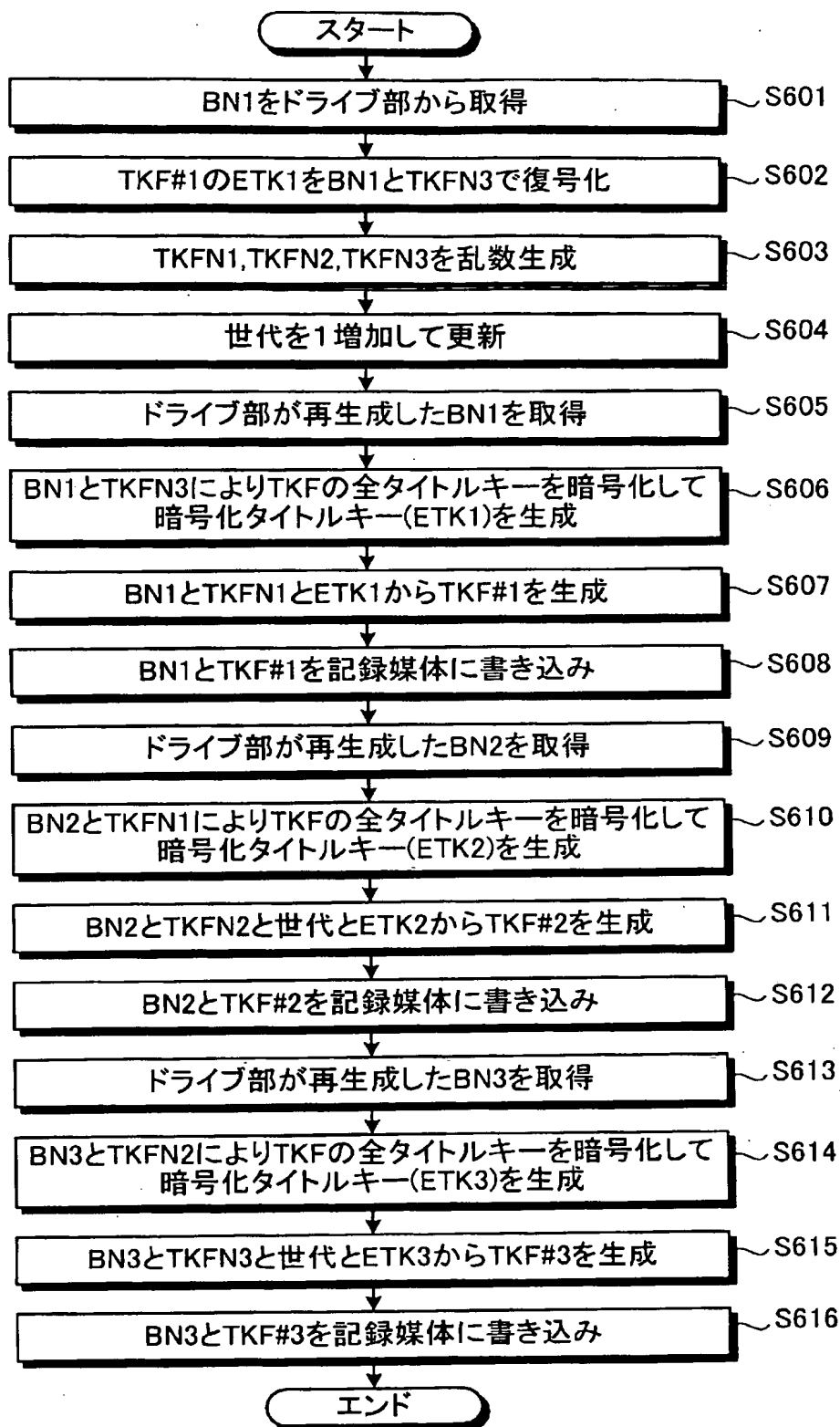
【図 4 - 2】



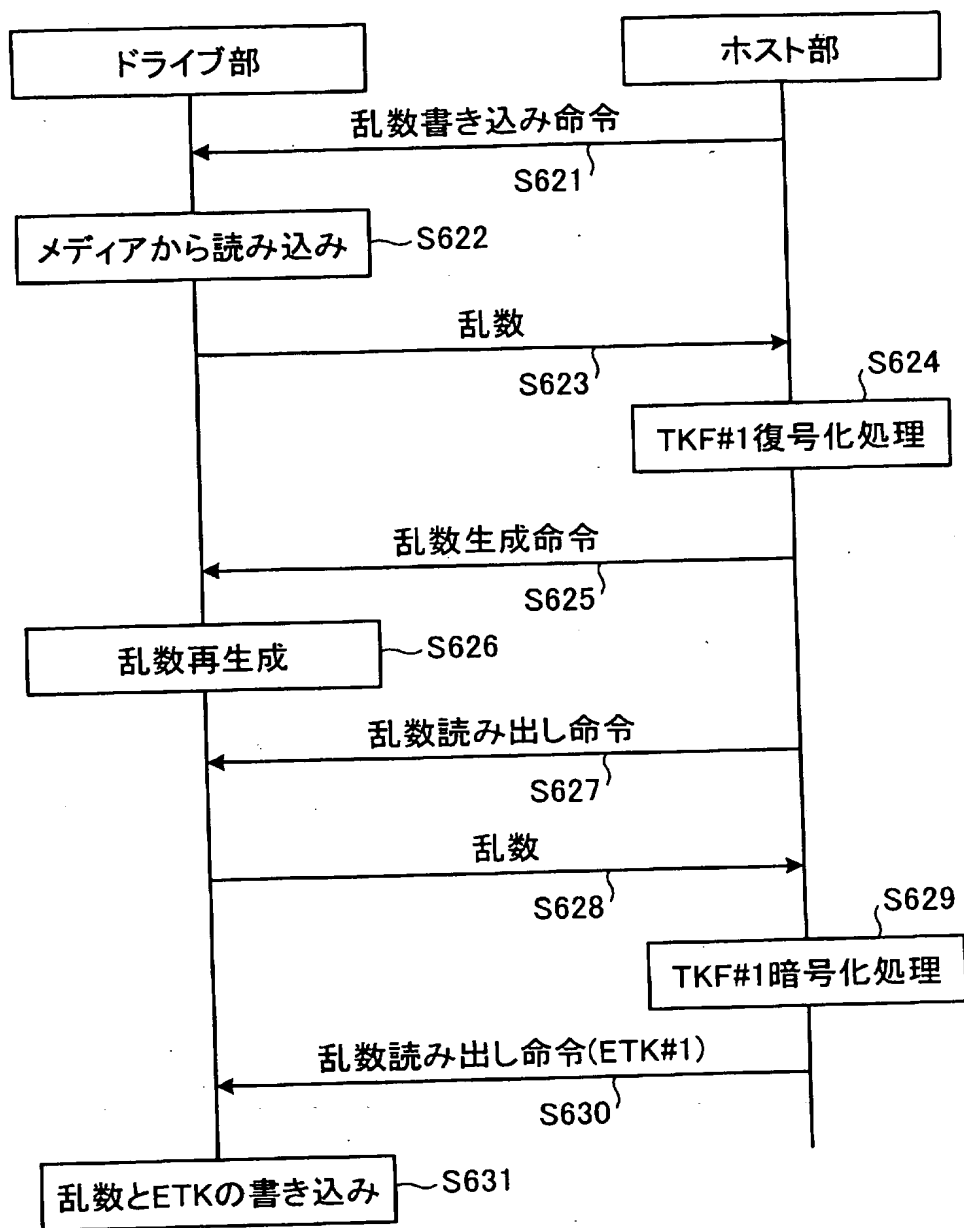
【図 5】



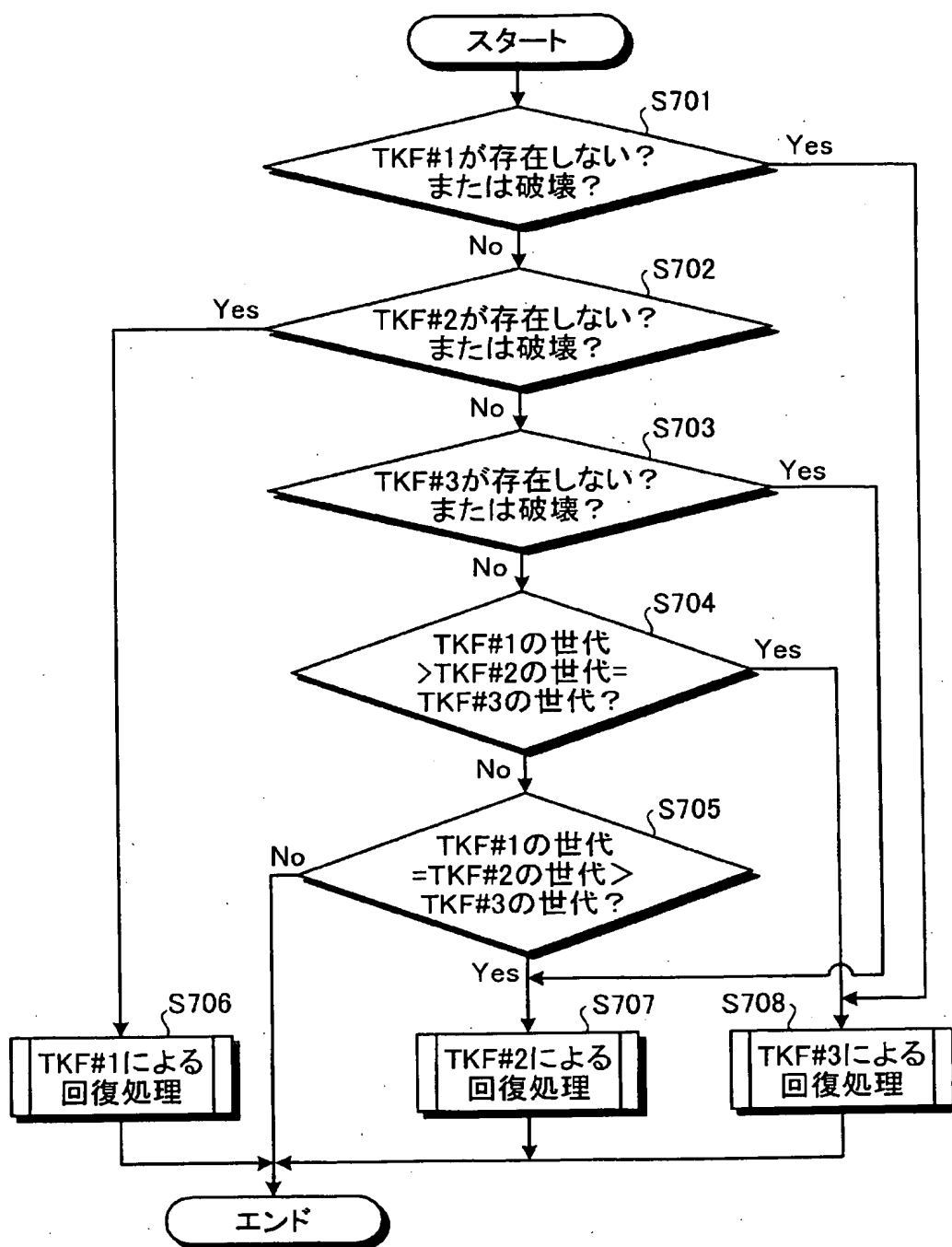
【図 6 - 1】



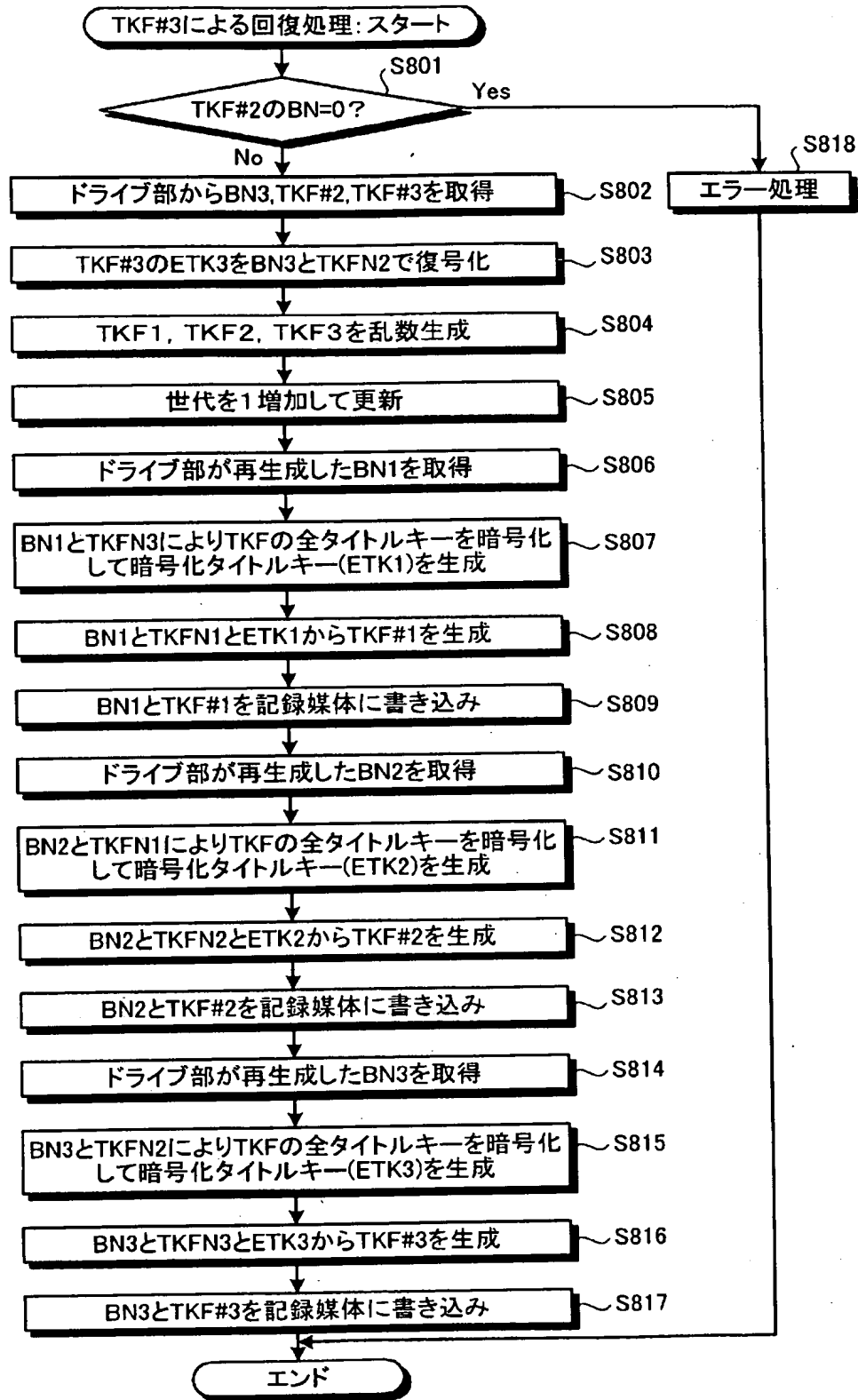
【図 6 - 2】



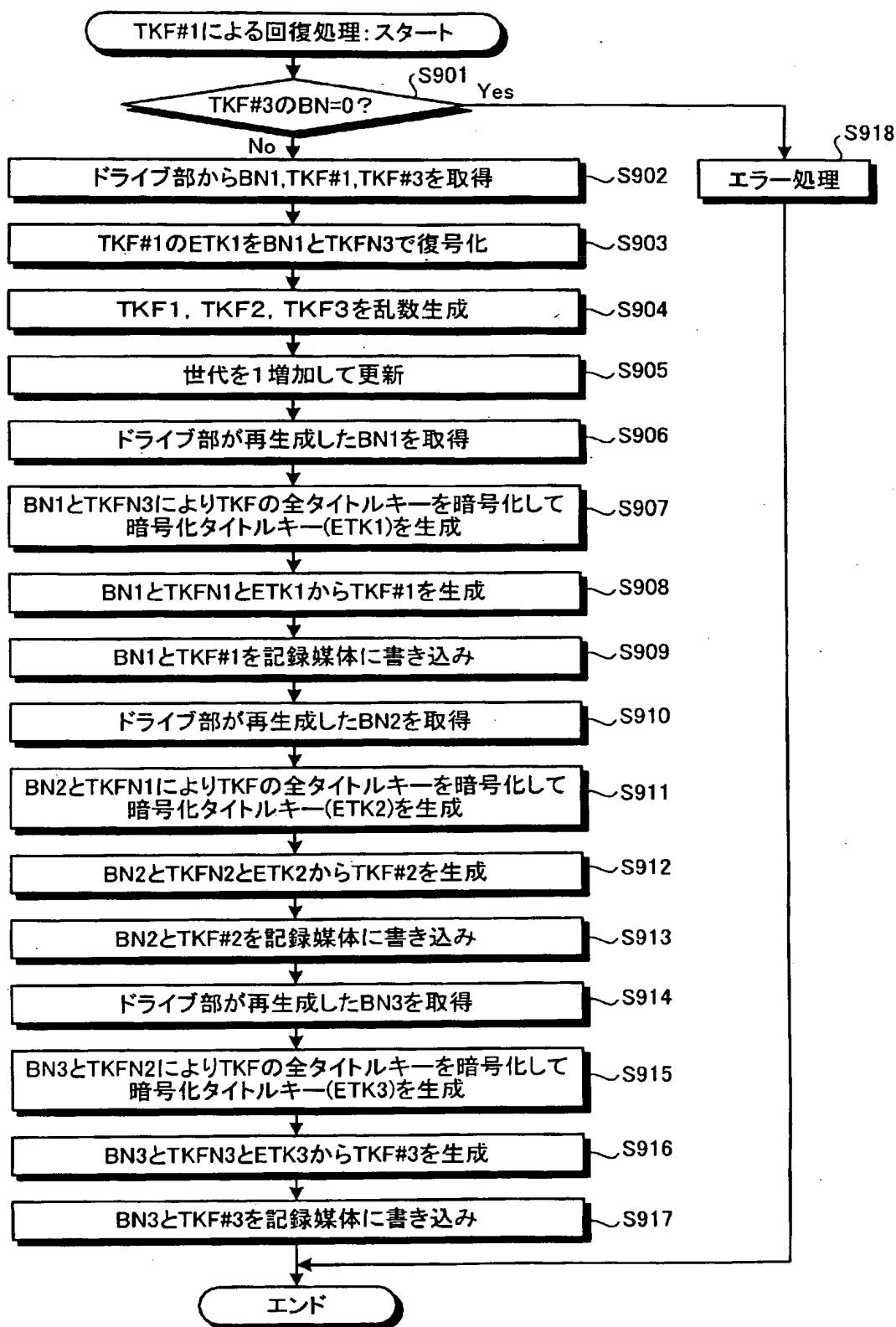
【図 7】



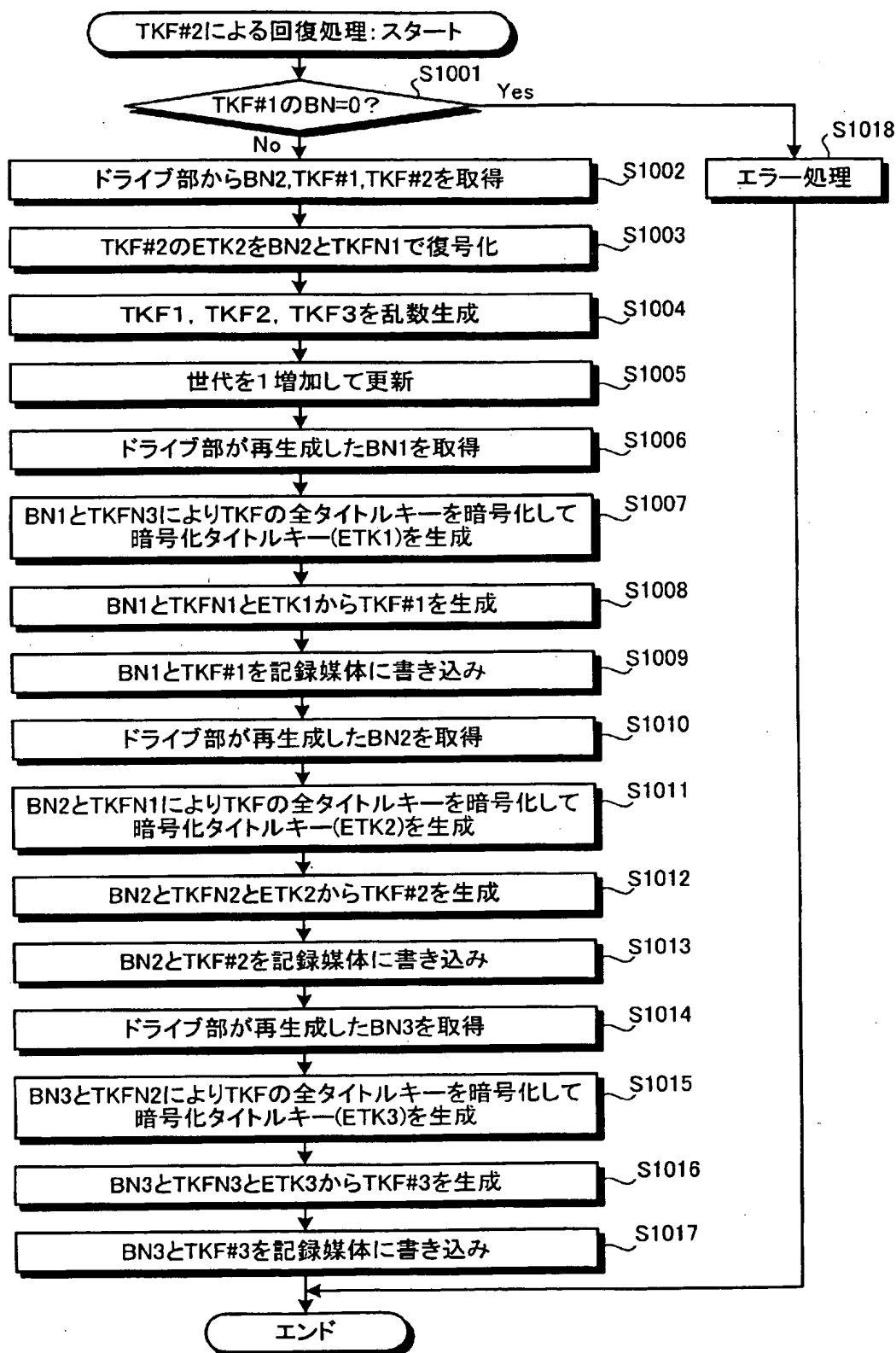
【図 8】



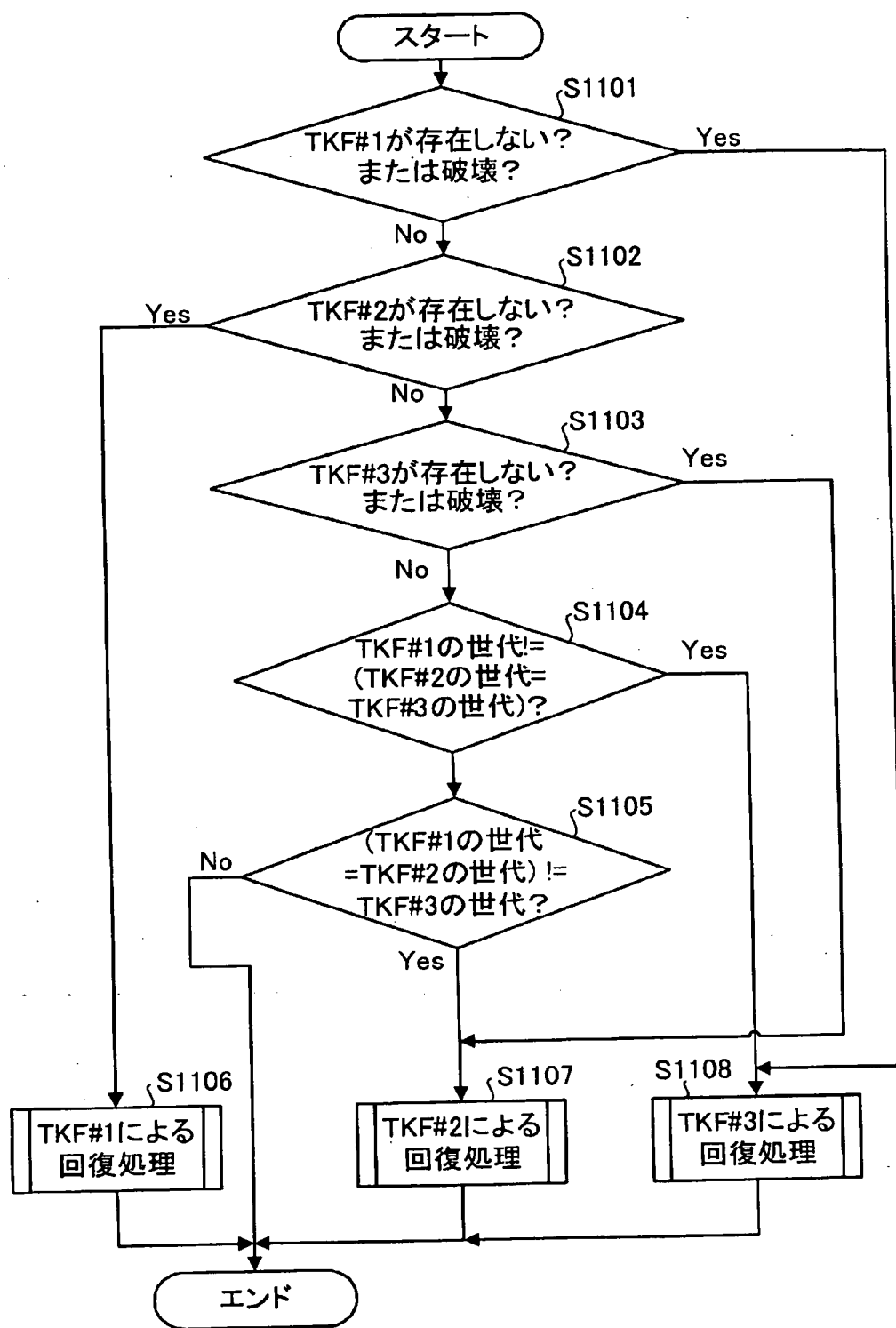
【図 9】



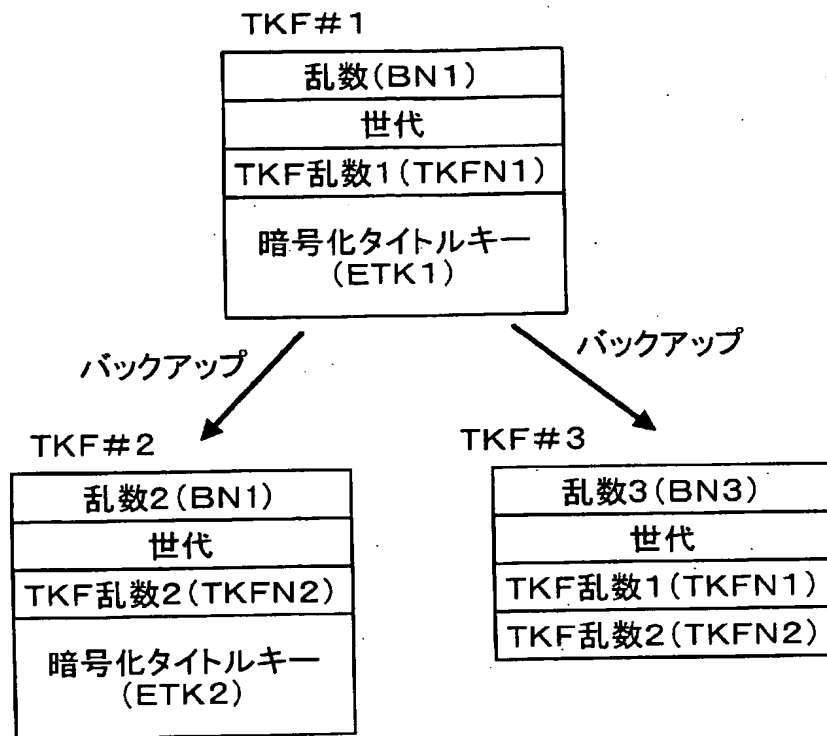
【図10】



【図 11】



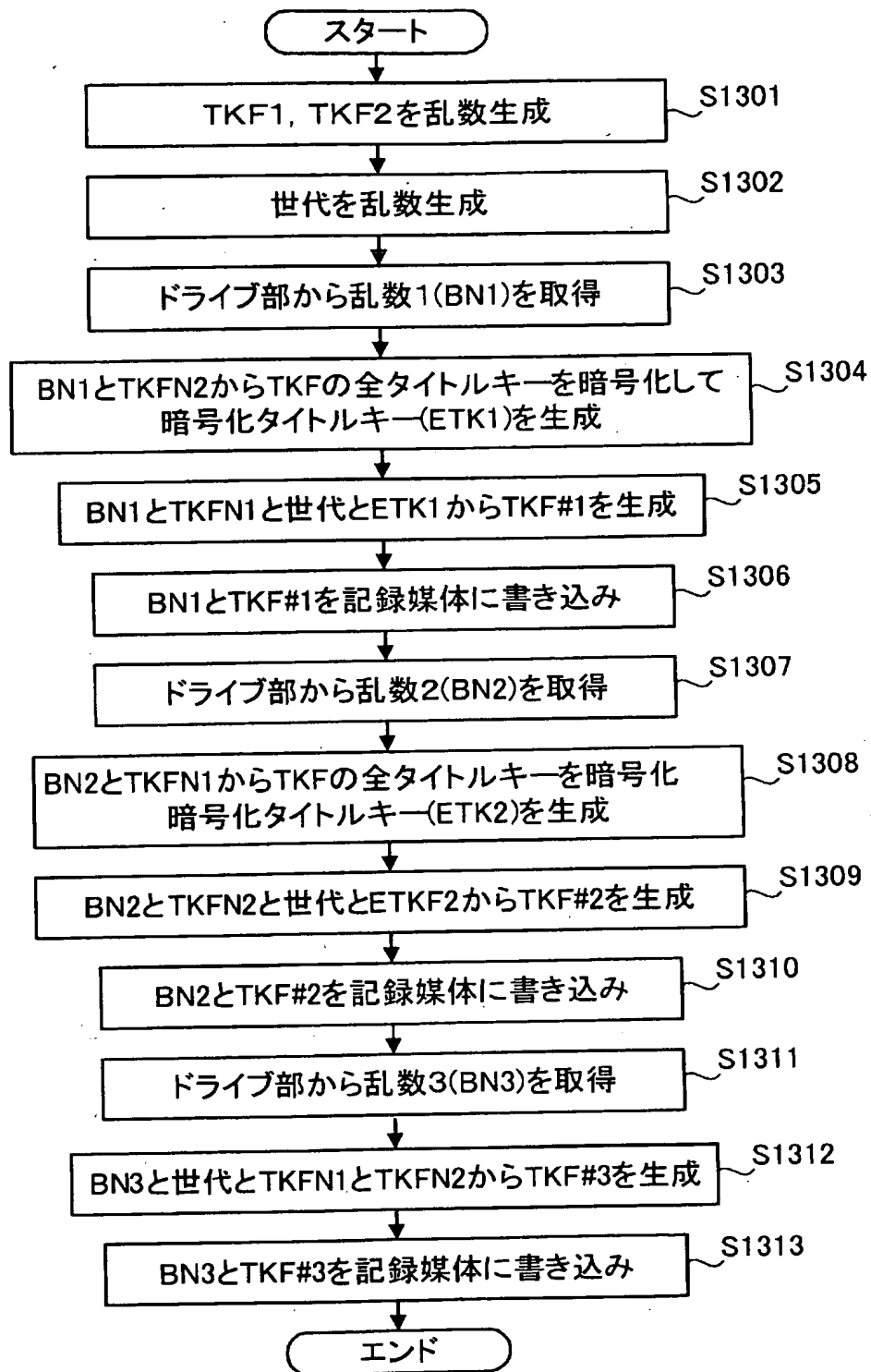
【図 1 2】



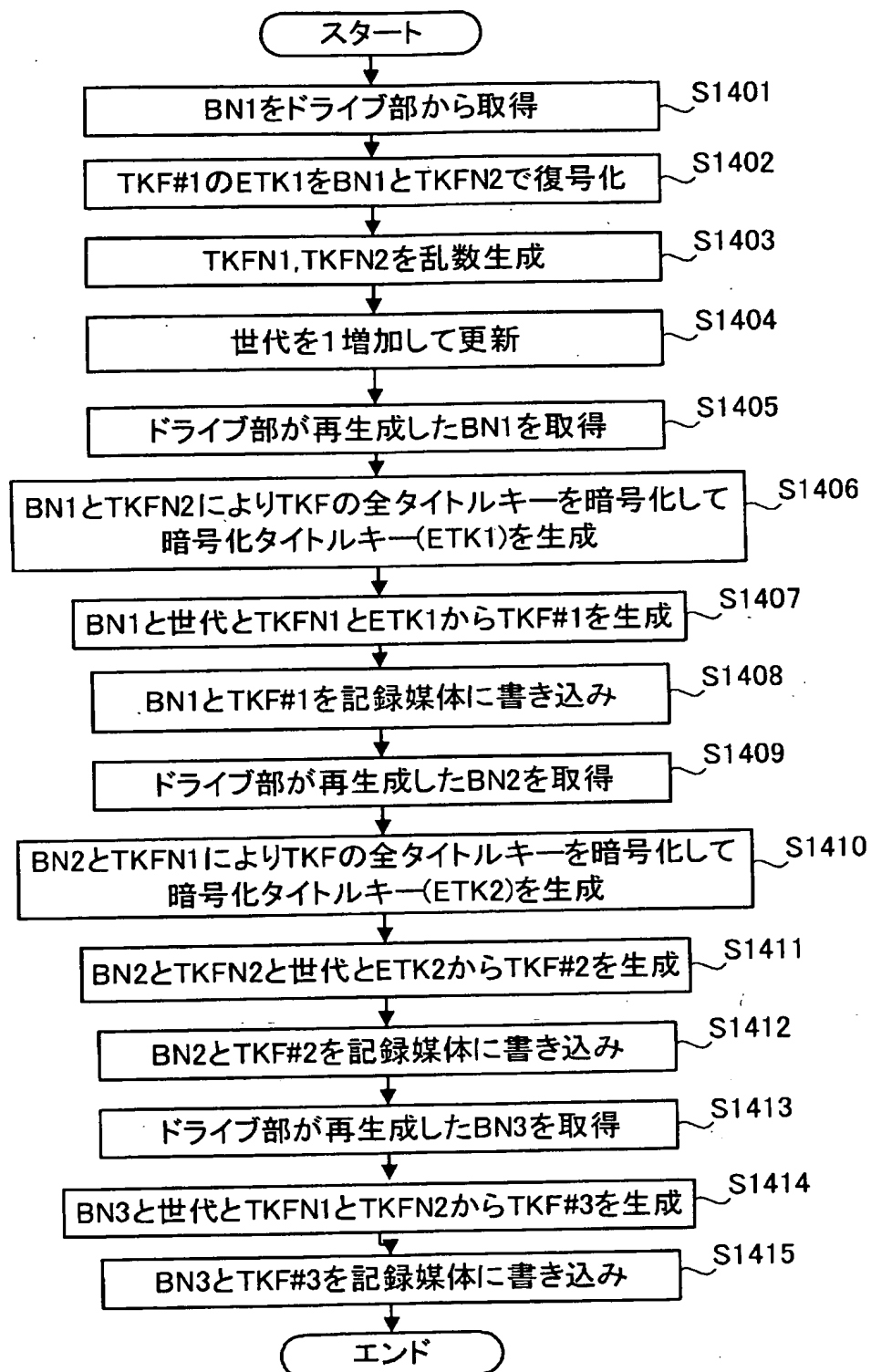
$$ETK1 = f(TK, BN1, TKFN2)$$

$$ETK2 = f(TK, BN2, TKFN1)$$

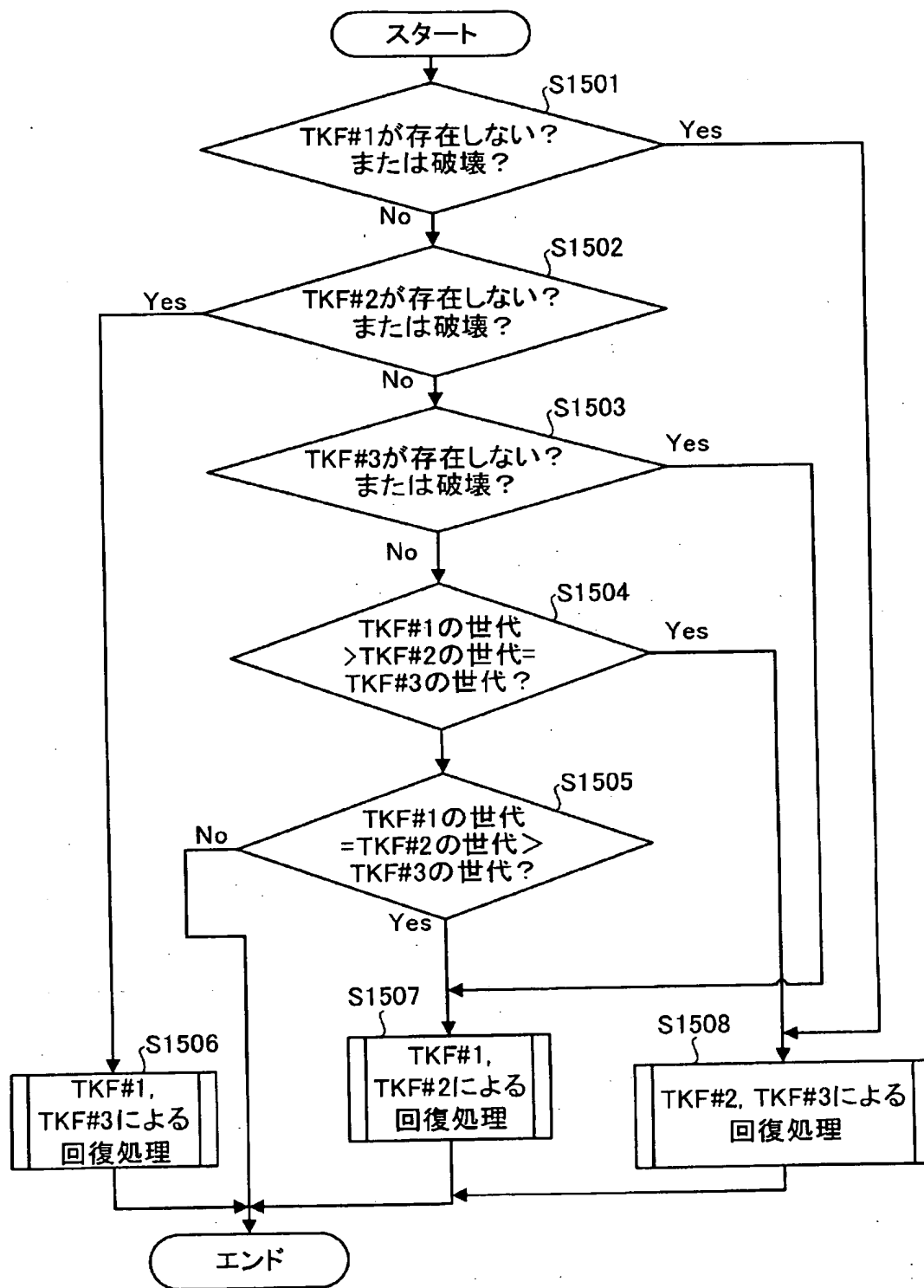
【図13】



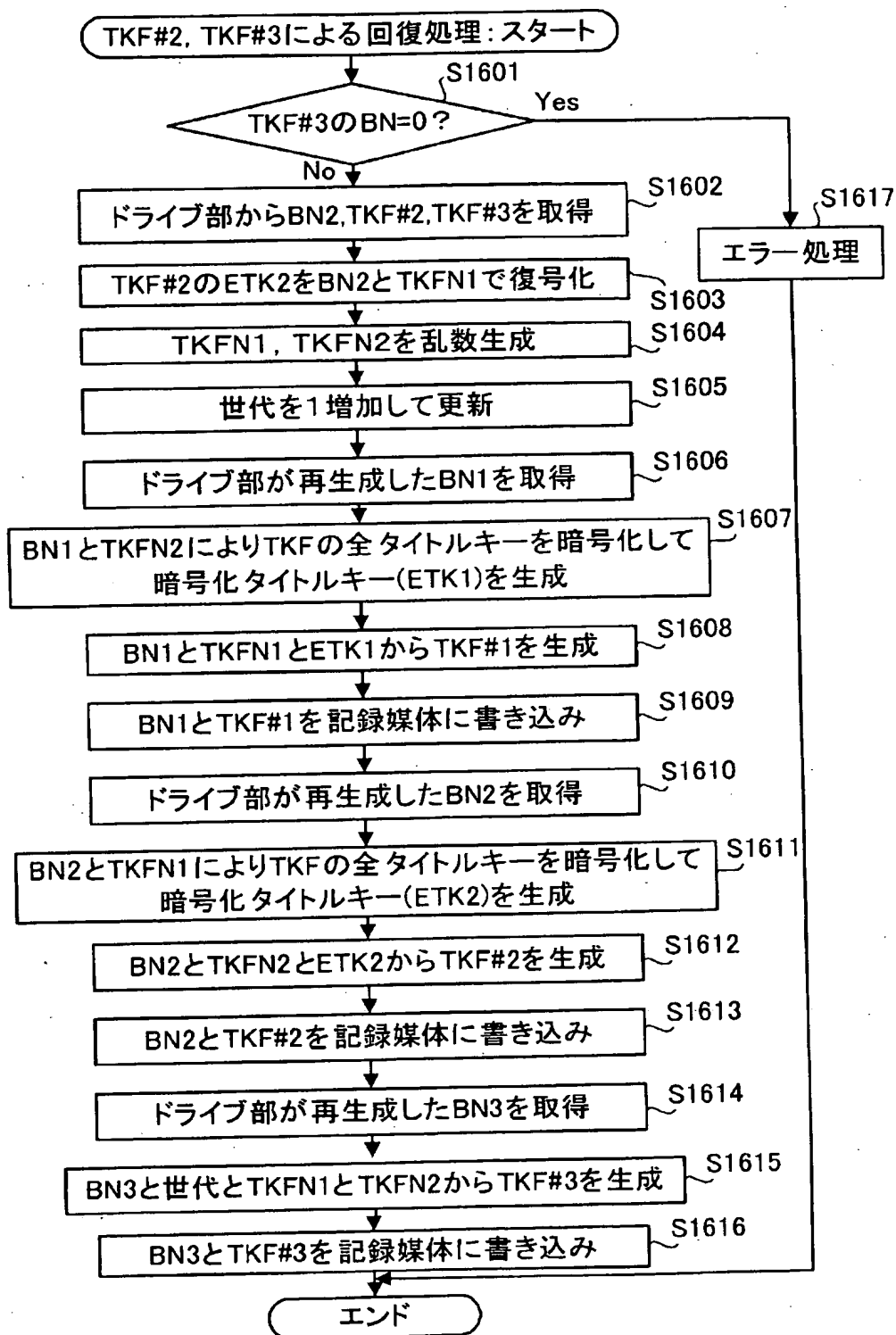
【図14】



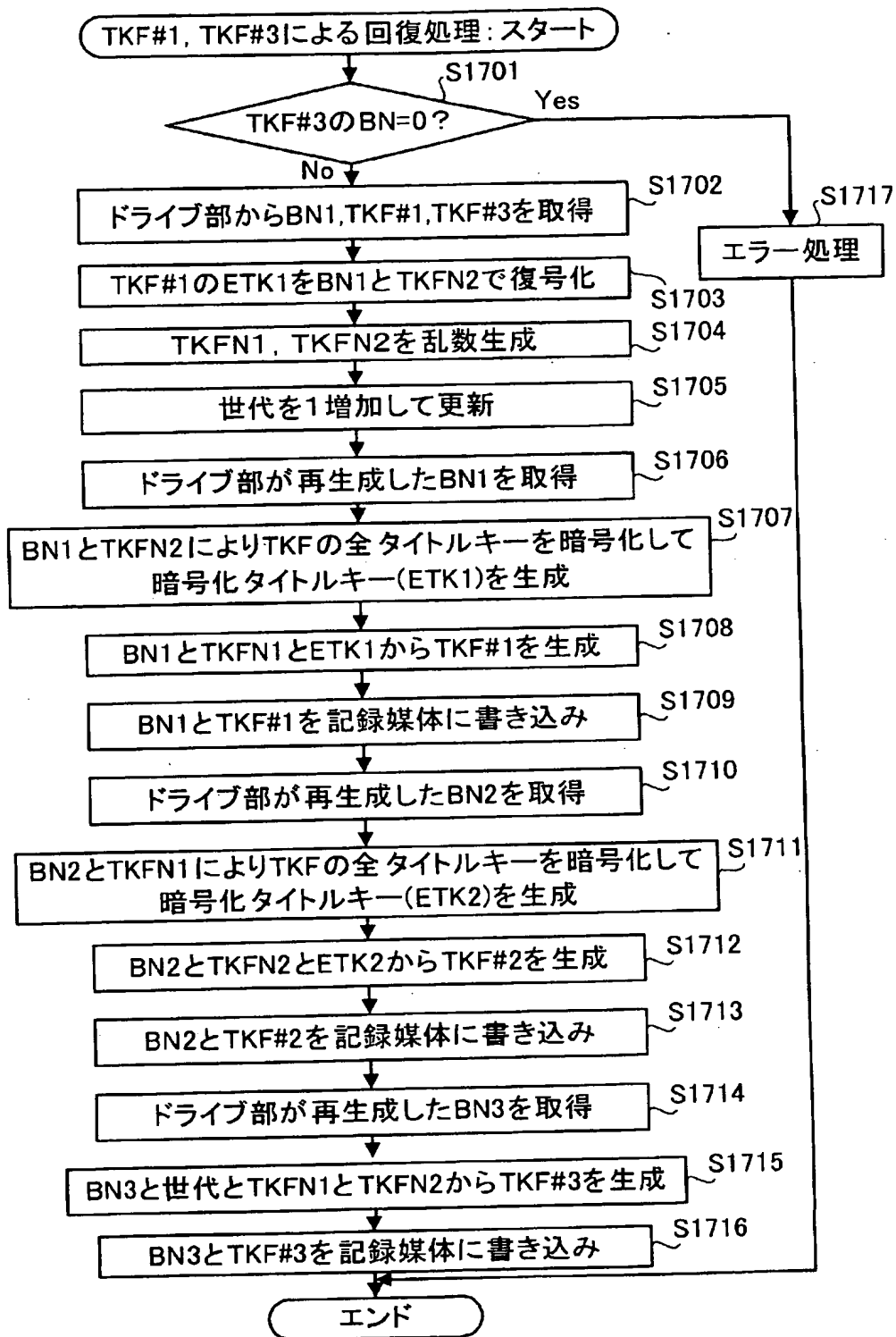
【図15】



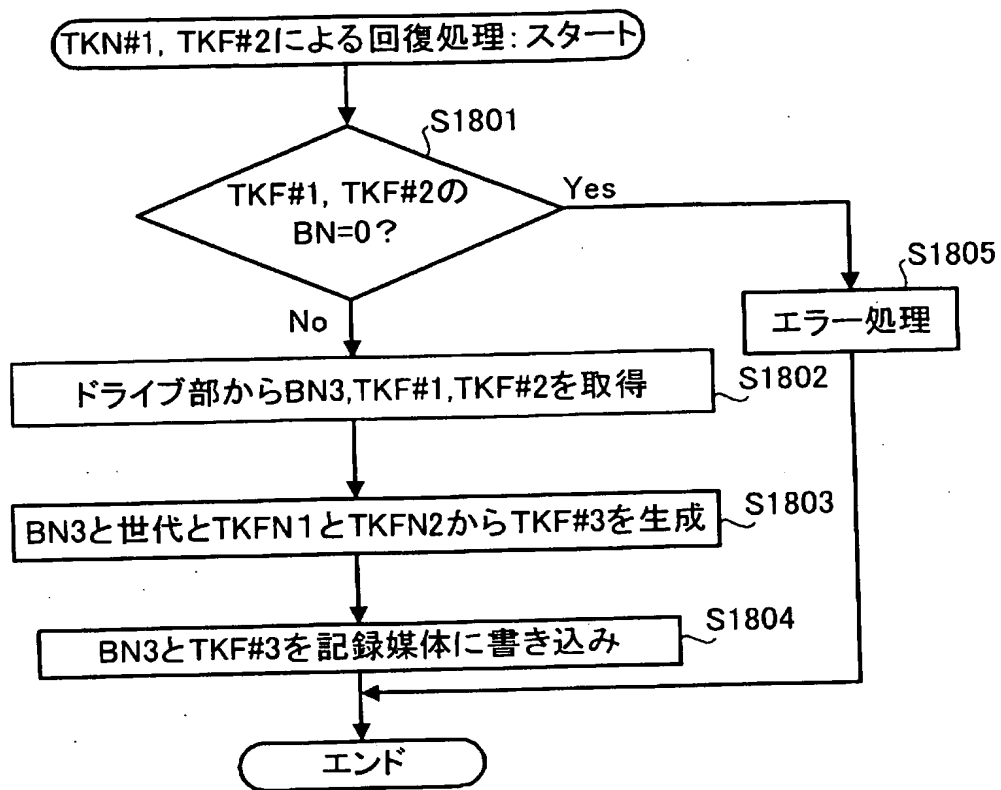
【図16】

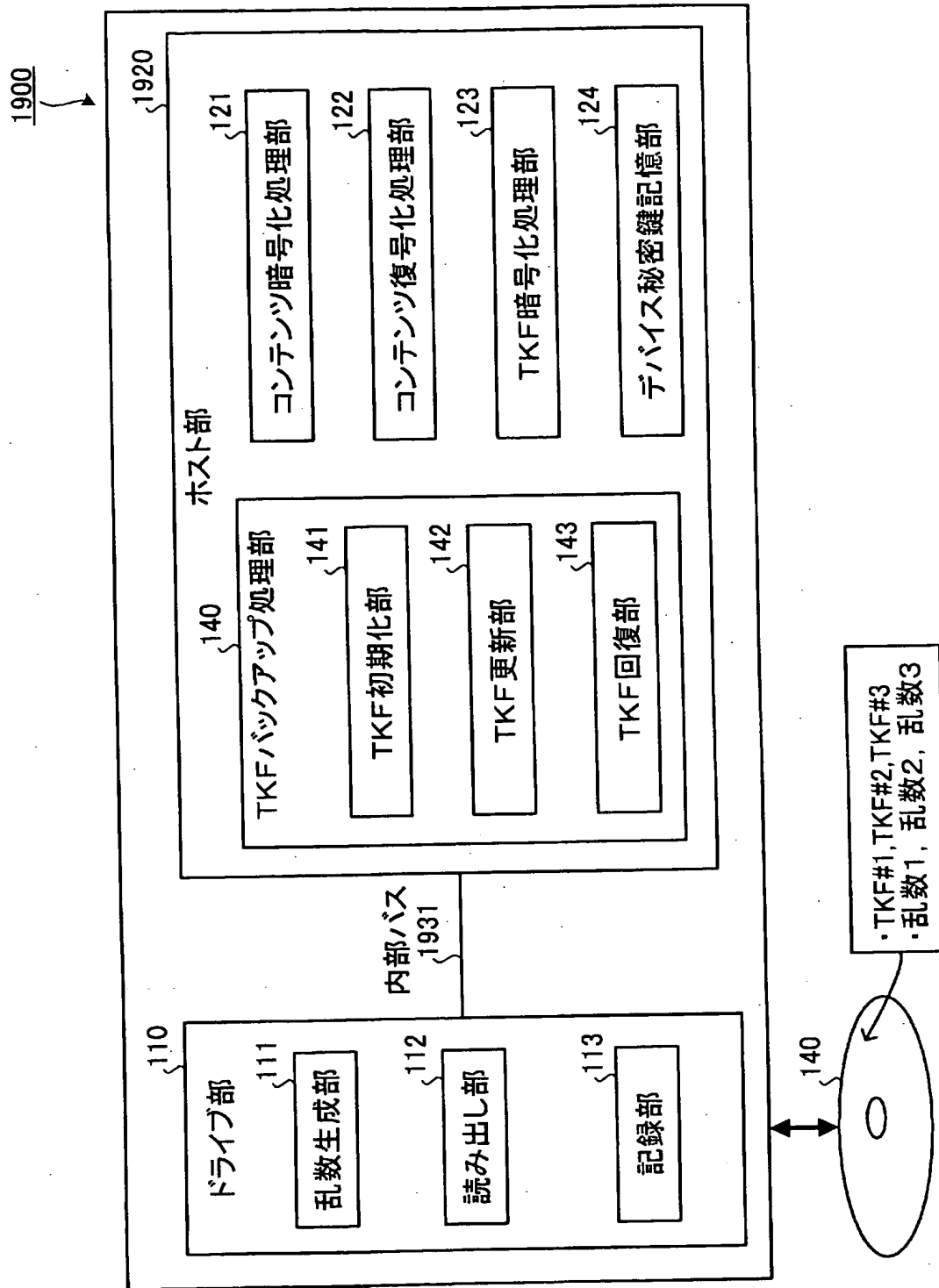


【図17】



【図18】





【書類名】 要約書

【要約】

【課題】 タイトルキーファイルの復元を確実にを行い、第三者によるコンテンツの不正な復元を防止すること。

【解決手段】 複数のタイトルコンテンツを暗号化するタイトルキーが登録されたタイトルキーファイルと、タイトルキーによって暗号化されたタイトルコンテンツとが記録された記録媒体の記録・再生を行うコンテンツ記録再生装置であって、タイトルキーファイルを生成して記録媒体に記録するTKF初期化部141と、複数のタイトルキーファイルのそれぞれに対応した第1の乱数を生成する乱数生成部111と、複数のタイトルキーファイルをDVDメディア140に記録する記録部113とを備え、TKF初期化部141は、タイトルキーファイルのそれぞれを、第1の乱数と関連づけられた他のタイトルキーファイルに登録された第2の乱数とによってタイトルキーを暗号化した暗号化タイトルキーと第1の乱数と第2の乱数とを登録する。

【選択図】 図1

出願人履歴

0 0 0 0 0 3 0 7 8

20010702

住所変更

5 9 9 1 3 7 0 1 3

東京都港区芝浦一丁目1番1号

株式会社東芝

3 0 1 0 6 3 4 9 6

20031101

住所変更

5 0 3 3 6 2 8 9 8

東京都港区芝浦一丁目1番1号

東芝ソリューション株式会社